

RINGS OF ALGEBRAIC NUMBERS IN INFINITE EXTENSIONS OF \mathbb{Q} AND ELLIPTIC CURVES RETAINING THEIR RANK.

ALEXANDRA SHLAPENTOKH

ABSTRACT. We show that elliptic curves whose Mordell-Weil groups are finitely generated over some infinite extensions of \mathbb{Q} , can be used to show the Diophantine undecidability of the rings of integers and bigger rings contained in some infinite extensions of rational numbers.

1. INTRODUCTION

The interest in the questions of existential definability and decidability over rings goes back to a question that was posed by Hilbert: given an arbitrary polynomial equation in several variables over \mathbb{Z} , is there a uniform algorithm to determine whether such an equation has solutions in \mathbb{Z} ? This question, otherwise known as Hilbert's 10th problem, has been answered negatively in the work of M. Davis, H. Putnam, J. Robinson and Yu. Matijasevich. (See [2], [3] and [8].) Since the time when this result was obtained, similar questions have been raised for other fields and rings. In other words, let R be a recursive ring. Then, given an arbitrary polynomial equation in several variables over R , is there a uniform algorithm to determine whether such an equation has solutions in R ? One way to resolve the question of Diophantine decidability negatively over a ring of characteristic 0 is to construct a Diophantine definition of \mathbb{Z} over such a ring. This notion is defined below.

Definition 1.1. Let R be a ring and let $A \subset R$. Then we say that A has a Diophantine definition over R if there exists a polynomial $f(t, x_1, \dots, x_n) \in R[t, x_1, \dots, x_n]$ such that for any $t \in R$,

$$\exists x_1, \dots, x_n \in R, f(t, x_1, \dots, x_n) = 0 \iff t \in A.$$

If the quotient field of R is not algebraically closed, we can allow a Diophantine definition to consist of several polynomials without changing the nature of the relation. (See [3] for more details.)

The usefulness of Diophantine definitions stems from the following easy lemma.

Lemma 1.2. *Let $R_1 \subset R_2$ be two recursive rings such that the quotient field of R_2 is not algebraically closed. Assume that Hilbert's Tenth Problem (abbreviated as "HTP" in the future) is undecidable over R_1 , and R_1 has a Diophantine definition over R_2 . Then HTP is undecidable over R_2 .*

Using norm equations, Diophantine definitions have been obtained for \mathbb{Z} over the rings of algebraic integers of some number fields. Jan Denef has constructed a Diophantine definition of \mathbb{Z} for the finite degree totally real extensions of \mathbb{Q} . Jan Denef and Leonard Lipshitz extended Denef's results to all the extensions of degree 2 of the finite degree totally real fields. Thanases Pheidas and the author of this paper have independently constructed Diophantine definitions of \mathbb{Z} for number fields with exactly one pair of non-real conjugate embeddings. Finally Harold N. Shapiro and the author of this paper showed that the subfields of all the fields mentioned above "inherited" the Diophantine definitions of \mathbb{Z} . (These subfields include all the abelian extensions.) The proofs of the results listed above can be found in [4], [5], [6], [14], [20], and [23].

The author modified the norm method to obtain Diophantine definitions of \mathbb{Z} for "large" subrings of totally real number fields (not equal to \mathbb{Q}) and their extensions of degree 2. (See [33], [26], [27], and [29].) Further, again using norm equations, the author also showed that in some totally real infinite algebraic extensions

2000 *Mathematics Subject Classification.* Primary 11U05; Secondary 11G05.

Key words and phrases. Hilbert's Tenth Problem, elliptic curve, Diophantine definition.

The research for this paper has been partially supported by NSF grant DMS-0354907 and ECU Faculty Senate Summer Research Grant.

of \mathbb{Q} and extensions of degree 2 of such fields one can give a Diophantine definition of \mathbb{Z} over the integral closures of “small” and “large” rings, though not over the rings of algebraic integers. (The terms “large” and “small” rings will be explained below.) Unfortunately, the norm method, at least in its present form, suffers from two serious limitations when used over infinite extensions: an “infinite part” of the extension has to have a non-splitting prime (effectively requiring working over an infinite cyclic extension), and one cannot use the method over the rings of algebraic integers. At the same time, though, one can describe rather easily at least one big class of fields to which the method applies, e. g. all Abelian extensions with finitely many ramified rational primes.

Another method of constructing Diophantine definitions uses elliptic curves. The idea of using elliptic curves for this purpose is due to Denef in [6] where he showed that the following proposition held.

Proposition 1.3. *Let K_∞ be a totally real algebraic possibly infinite extension of \mathbb{Q} . If there exists an elliptic curve \mathbf{E} over \mathbb{Q} such that $[\mathbf{E}(K) : \mathbf{E}(\mathbb{Q})] < \infty$, then \mathbb{Z} has a Diophantine definition over O_K .*

Expanding Denef’s ideas, Bjorn Poonen proved the following result in [16].

Theorem 1.4. *Let M/K be a number field extension with an elliptic curve \mathbf{E} defined over K , of rank one over K , such that the rank of \mathbf{E} over M is also one. Then O_K (the ring of integers of K) is Diophantine over O_M .*

Cornelissen, Pheidas and Zahidi weakened somewhat assumptions of Poonen’s theorem. Instead of requiring a rank 1 curve retaining its rank in the extension, they require existence of a rank 1 elliptic curve over the bigger field and an abelian variety over the smaller field retaining its rank in the extension (see [1]). Further, Poonen and the author have independently shown that the conditions of Theorem 1.4 can be weakened to remove the assumption that rank is one and require only that the rank in the extension is positive and is the same as the rank below (see [22] and [15]). In [22] the author also showed that the elliptic curve technique can be used over large rings.

Elliptic curves of rank one have also been used to construct Diophantine models of \mathbb{Z} (an alternative method for showing Diophantine undecidability of a ring) over “very large” rings of rational and algebraic numbers, as well as to construct infinite discrete in a p -adic and/or an archimedean topology Diophantine sets over these rings. (See [17] and [18].) The interest in such sets has been motivated by a series of conjectures by Barry Mazur (see [9], [10], [11] and [12]) and their variations (see [30]).

In this paper we explore to what extent the elliptic curve methods can be adapted for showing the Diophantine undecidability of rings of algebraic numbers (including rings of integers) in infinite extensions. If one uses elliptic curves instead of norm equations to construct Diophantine definitions over an infinite extension, in principle, one does not need cyclic extensions and it is possible to work over rings of integers. The difficulties will lie along a different plane: the elliptic curve method requires existence of an elliptic curve of positive rank with a finitely generated Mordell-Weil group over an infinite extension. While we already have plenty of examples of this sort, the general situation is far from clear. (See [13] for more details.)

Another technical difficulty which occurs over infinite extensions is connected to defining bounds on the height of the elements. Using quadratic forms and divisibility we can solve the problem to large extent over totally real fields and to some extent over extensions of degree 2 of totally real fields.

In this paper we refine our results on bounds as used in [25], [31], and [33]. We also generalize Denef’s results to any totally real infinite extension K_∞ of \mathbb{Q} and any of its extensions of degree 2 assuming some finite extension of K_∞ has an elliptic curve of positive rank with a finitely generated Mordel-Weil group. We will be able to treat rings of integers as well as “large” rings in these extensions.

We will also show that if there exists an elliptic curve of rank 1 with a finitely generated Mordel-Weil group in an infinite extension, then techniques from [17] and [18] are adaptable for this situation to reach similar results. Please note that for this application we will not need bound equations and thus the discussion can take place over an arbitrary infinite algebraic extension of \mathbb{Q} .

2. PRELIMINARY RESULTS, DEFINITIONS AND THE STATEMENT OF THE MAIN THEOREM.

In this section we state some technical propositions which will be used in the proofs and describe notation and assumptions to be used in the sections below. We start with the proposition on definability of integrality at finitely many primes over number fields.

Proposition 2.1. *Let K be a number field. Let \mathcal{W}_K be any set of primes of K . Let $\mathcal{S}_K \subseteq \mathcal{W}_K$ be a finite set. Let $\mathcal{V}_K = \mathcal{W}_K \setminus \mathcal{S}_K$. Then O_{K, \mathcal{V}_K} has a Diophantine definition over O_{K, \mathcal{W}_K} . (See, for example, [24].)*

“Infinite” versions of this proposition are more complicated. Before stating some of them below we introduce new terminology.

Notation and Assumptions 2.2. The following terminology will be used in the rest of the paper.

- Let L be an algebraic, possibly infinite extension of \mathbb{Q} . Let Z be a number field contained in L . Let \mathcal{C}_Z be a finite set of primes of Z . Assume further that there exists a polynomial $I_{\mathcal{C}_Z/L}(x, t_1, \dots, t_k) \in Z[x, t_1, \dots, t_k]$ such that

$$(2.1) \quad I_{\mathcal{C}_Z/L}(x, t_1, \dots, t_k) = 0$$

has solutions in L only if $u_{\mathcal{C}_Z/L}x$ is integral at all the primes of \mathcal{C}_Z , where $u_{\mathcal{C}_Z/L} \in \mathbb{Z}_{>0}$ is fixed and depends only on \mathcal{C}_Z . Assume also that if $x \in Z$ and is integral at all the primes of \mathcal{C}_Z , then (2.1) has solutions in Z . Then we will call \mathcal{C}_Z -primes L -boundable. If we can set $u_{\mathcal{C}_Z/L} = 1$, then we will say that *integrality is definable* at primes of \mathcal{C}_Z over L .

- Let L , as above, be an algebraic, possibly infinite extension of \mathbb{Q} . Let q be a rational prime. Then let the *degree index* of q (with respect to L) denoted by $i_L(q)$ be defined as follows:

$$i_L(q) = \max\{n \in \mathbb{Z}_{\geq 0} : n = \text{ord}_q[M : \mathbb{Q}], \text{ where } M \text{ is a number field contained in } L\}$$

The following statement is taken from Section 3 of [33].

Proposition 2.3. *Let L be an algebraic, possibly infinite extension of \mathbb{Q} . Let Z be a number field contained in L such that L is normal over Z . Let \mathcal{C}_Z be a finite set of primes of Z such that for every $\mathfrak{p}_Z \in \mathcal{C}_Z$ the following conditions are satisfied.*

- *There exists a non-negative integer m_f such that any prime lying above \mathfrak{p}_Z in a number field contained in L has a relative degree f over Z with $\text{ord}_q f \leq m_f$.*
- *There exists a non-negative integer m_e such that any prime lying above \mathfrak{p}_Z in a number field contained in L has a ramification degree e over Z with $\text{ord}_q e \leq m_e$.*

Then \mathcal{C}_Z -primes are L -boundable. If we also assume that the ramification degree for all the factors of primes in \mathcal{C}_Z is bounded from above, then integrality at all the primes of \mathcal{C}_Z is definable.

Finally we want to separate out a case which occurs quite often in our discussion of infinite extensions.

Corollary 2.4. *Suppose L is a normal, algebraic, possibly infinite extension of some number field such that for some odd rational prime q the degree index of q with respect to L is finite. Then for any number field $M \subset L$, any M -prime \mathfrak{p}_M is L -boundable.*

Notation and Assumptions 2.5. Next we introduce several additional notational conventions to be used throughout the paper.

- Let N be any finite extension of a number field U . Let \mathcal{T}_U (or $\mathcal{V}_U, \mathcal{W}_U, \mathcal{S}_U, \mathcal{E}_U, \mathcal{N}_U, \mathcal{L}_U, \mathcal{R}_U, \dots$) be any set of primes of U . Then let \mathcal{T}_N (or $\mathcal{V}_N, \mathcal{W}_N, \mathcal{S}_N, \mathcal{E}_N, \mathcal{N}_N, \mathcal{L}_N, \mathcal{R}_N, \dots$) be the set of all primes of N lying above the primes of \mathcal{T}_U .
- If N_∞ is an algebraic, possibly infinite extension of U , then $O_{N_\infty, \mathcal{T}_{N_\infty}}$ (or $O_{N_\infty, \mathcal{V}_{N_\infty}}, O_{N_\infty, \mathcal{W}_{N_\infty}}, \dots$) will denote the integral closure of O_{U, \mathcal{T}_U} in N_∞ (or respectively of $O_{U, \mathcal{V}_U}, O_{U, \mathcal{W}_U}, \dots$).
- For any number field U let $\mathcal{P}(U)$ denote the set of all non-archimedean primes of U .
- For any field U and a set $\mathcal{W}_U \subset \mathcal{P}(U)$, let $\overline{\mathcal{W}}_U$ be the closure of \mathcal{W}_U with respect to conjugation over \mathbb{Q} .
- For any field U and a set $\mathcal{W}_U \subset \mathcal{P}(U)$, let $\hat{\mathcal{W}}_U$ be a subset of \mathcal{W}_U obtained from \mathcal{W}_U by removing a prime of highest relative degree over \mathbb{Q} from every complete set of \mathbb{Q} -conjugates contained in \mathcal{W}_U .

- We will assume that all the fields under discussion are subfields of \mathbb{C} . Given two fields $U, T \subset \mathbb{C}$ we will interpret UT to mean the smallest subfield of \mathbb{C} containing both fields.
- For a number field K we will denote its Galois closure over \mathbb{Q} by K^{Gal} .

Below we state two well-known technical propositions which are also quite important for the proofs in this paper.

Proposition 2.6. *Let K be a number field. Let \mathcal{W}_K be any set of primes of K . Then the set of non-zero elements of O_{K, \mathcal{W}_K} has a Diophantine definition over O_{K, \mathcal{W}_K} . (See, for example, [24].)*

This proposition allows us to use variables which take values in K while we are “officially” working with variables taking values in O_{K, \mathcal{W}_K} . We write these K -variables as ratios of variables in O_{K, \mathcal{W}_K} with the proviso that the denominator is not zero.

The next proposition allows us to establish some bounds on real valuations. It is due to Denef and can be found in [5] or Section 5.1 of [32].

Proposition 2.7. *Let K_∞ be a totally real algebraic possibly infinite extension of \mathbb{Q} . Let G_∞ be a finite extension of K_∞ generated by an element $\alpha \in K_\infty$. Then the set $\{x \in G_\infty : \sigma(x) \geq 0 \ \forall \sigma : G_\infty \longrightarrow \mathbb{R}\}$ is Diophantine over G_∞ .*

The following proposition allows us to avoid certain sets of primes in the numerators and can be derived from Proposition 25, Section 8, Chapter I of [7].

Lemma 2.8. *Let T/K be a number field extension. Let $R(X)$ be the monic irreducible polynomial of an integral generator of T over K . Let \mathcal{V}_K be the set of all primes of K without relative degree one factors in T and not dividing the discriminant of $R(X)$. Then for all $x \in K$ and all $\mathfrak{p} \in \mathcal{V}_K$ we have that $\text{ord}_{\mathfrak{p}} R(x) \leq 0$.*

The next lemma will allow us to conclude that under some circumstances the set of primes we can prevent from appearing in the numerators of the divisors of the elements is closed under conjugation over \mathbb{Q} .

Lemma 2.9. *Let $T, K, R(X)$ be as in Lemma 2.8. Let T_0 be a finite extension of \mathbb{Q} and assume that $T = T_0 K$. Assume further that $[T_0 : \mathbb{Q}] = [T : K] \geq 2$, T/\mathbb{Q} is Galois, and $[K : \mathbb{Q}]$ is Galois. Suppose that for some prime \mathfrak{p}_K of K we have that for all $x \in K$ it is the case that $\text{ord}_{\mathfrak{p}_K} R(x) \leq 0$. Then for any $\bar{\mathfrak{p}}_K$ -conjugate of \mathfrak{p}_K over \mathbb{Q} , for all $x \in K$, we have that $\text{ord}_{\bar{\mathfrak{p}}_K} R(x) \leq 0$.*

Proof. The lemma follows almost immediately from the fact that $R(X)$, the monic irreducible polynomial of an integral generator of T over K , can be assumed to have rational integer coefficients. \square

We generalize this result for some classes of infinite extensions.

Lemma 2.10. *Let $T, T_0, K, R(X), \mathcal{V}_K$ be as in Lemmas 2.8 and 2.9, assume that $[T_0 : \mathbb{Q}] > 2$ and T/K is Galois. Let K_∞ be a normal possibly infinite extension of K such that for any number field $N \subset K_\infty$ with $K \subseteq N$, we have that $([N : K], [T : K]) = 1$. (Observe that this condition implies by Proposition 2.3 that any finite set of primes of K is boundable over K_∞ .) Let \mathcal{W}_K be the set of all primes of K without degree one factors in T . Let \mathcal{S}_K be any finite set of primes of K . Let $\mathcal{E}_K = (\mathcal{W}_K \cup \mathcal{S}_K) \setminus \mathcal{V}_K$. Let μ - a generator of T_0 over \mathbb{Q} and T over K be an integral unit. Let $a \in \mathbb{Z}_{>0}$ be an integer divisible by all the primes in \mathcal{E}_K . Let $M \subset K_\infty$ be any number field containing K and the values of all the variables below. Finally assume that the following equations hold over K_∞ .*

$$(2.2) \quad \begin{cases} I_{\mathcal{E}_K/K_\infty}(x, t_1, \dots, t_k) = 0 \\ y = R(u_{\mathcal{E}_K/K_\infty} x) \end{cases}$$

Then for any $\mathfrak{p}_M \in \mathcal{W}_M \cup \mathcal{S}_M$ we have that $\text{ord}_{\mathfrak{p}_M} y \leq 0$.

Proof. Without loss of generality we can assume that M/K is a Galois extension. (If not we can take the Galois closure of M over K contained in K_∞ .) Next by Lemma 11.2 we have that no prime \mathfrak{p}_M of M has a relative degree one factor in MT . Thus for all primes $\mathfrak{p}_M \in \mathcal{W}_M \setminus \mathcal{E}_M$ we have that $\text{ord}_{\mathfrak{p}_M} y \leq 0$. Next we proceed to the primes of \mathcal{E}_M . By definition of $I_{\mathcal{E}_K/K_\infty}(x, t_1, \dots, t_k)$ and $u_{\mathcal{E}_K/K_\infty}$ we have that for any $\mathfrak{q}_M \in \mathcal{E}_M$ it is the case that $\text{ord}_{\mathfrak{q}_M} u_{\mathcal{E}_K/K_\infty} x \geq 0$. Thus by choice of a we also have that $\text{ord}_{\mathfrak{q}_M} a u_{\mathcal{E}_K/K_\infty} x > 0$. Since μ is an integral unit, the free term of $R(X)$ is ± 1 and thus $R(a u_{\mathcal{E}_K/K_\infty} x) \equiv \pm 1 \pmod{\mathfrak{q}_M}$. \square

To state the main theorem of the paper we need the following definitions.

Definition 2.11. Let K be a number field and let $\mathcal{W}_K \subset \mathcal{P}(K)$. Let $O_{K, \mathcal{W}_K} = \{x \in K : \text{ord}_{\mathfrak{p}} x \geq 0 \ \forall \mathfrak{p} \notin \mathcal{W}_K\}$. Then call O_{K, \mathcal{W}_K} a *small* ring if \mathcal{W}_K is finite. If \mathcal{W}_K is infinite, then call the ring *big* or *large*. If K_∞ is an infinite algebraic extension of K , then call the integral closure of a small subring of K in K_∞ *small*, and call the integral closure of a big subring of K in K_∞ *big*.

Remark 2.12. Note that if $\mathcal{W}_K = \emptyset$, then $O_{K, \mathcal{W}_K} = O_K$ is the ring of integers of K , and if $\mathcal{W}_K = \mathcal{P}(K)$, then $O_{K, \mathcal{W}_K} = K$. The small rings are also known as “rings of \mathcal{S} -integers”. Observe that the integral closure of a small ring in a finite extension is also small, and similarly, the integral closure of a big ring in a finite extension is also big.

Definition 2.13. Let K_∞ be an algebraic possibly infinite extension of \mathbb{Q} . Let R be a small subring of K_∞ . Suppose now that there exists a number field K contained in K_∞ and finite set of primes \mathcal{S}_K of K such that $R = O_{K_\infty, \mathcal{S}_K}$ and all the primes of \mathcal{S}_K are either boundable in K_∞ or integrality at all the primes of \mathcal{S}_K is definable over K_∞ , then we will say that the set of primes occurring in the denominators of the divisors of elements of R is boundable or that integrality is definable at the primes occurring in the denominators of divisors of the elements of R .

We are now ready to state the main theorems of our paper.

Main Theorem A. Let K_∞ be a totally real possibly infinite algebraic extension of \mathbb{Q} . Let U_∞ be a finite extension of K_∞ such that there exists an elliptic curve \mathbf{E} defined over U_∞ with $\mathbf{E}(U_\infty)$ finitely generated and of a positive rank. Then \mathbb{Z} is existentially definable and HTP is unsolvable over the ring of integers of K_∞ . (See Theorem 5.4.)

Main Theorem B. Let K_∞, U_∞ and \mathbf{E} be as above. Let G_∞ be an extension of degree two of K_∞ . If G_∞ has no real embeddings into its algebraic closure, assume additionally that K_∞ has a totally real extension of degree two. Then \mathbb{Z} is existentially definable and HTP is unsolvable over the ring of integers of G_∞ . (See Theorem 7.9.)

Main Theorem C. Let K_∞ be a totally real possibly infinite algebraic extension of \mathbb{Q} , normal over some number field and with a finite degree index for some odd rational prime number p . Let U_∞ be a finite extension of K_∞ such that there exists an elliptic curve \mathbf{E} defined over U_∞ with $\mathbf{E}(U_\infty)$ finitely generated and of a positive rank. Then

- (1) K_∞ contains a large subring R such that \mathbb{Z} is definable over R and HTP is unsolvable over R .
- (2) For any small subring R of K_∞ we have that \mathbb{Z} is definable over R and HTP is unsolvable over R .

(See Theorems 6.9 and 6.13.)

Main Theorem D. Let K_∞ be a totally real possibly infinite algebraic extension of \mathbb{Q} normal over some number field and such that there exist infinitely many rational prime numbers of finite degree index with respect to K_∞ . Let U_∞ be a finite extension of K_∞ such that there exists an elliptic curve \mathbf{E} defined over U_∞ with $\mathbf{E}(U_\infty)$ finitely generated and of a positive rank. Then for any $\varepsilon > 0$ we have that K_∞ contains a large subring R satisfying the following conditions:

- (1) There exists a number field $K \subset K_\infty$ and a set $\mathcal{W}_K \subset \mathcal{P}(K)$ of (Dirichlet or natural) density greater than $1 - \varepsilon$ such that $R = O_{K_\infty, \mathcal{W}_K}$.
- (2) \mathbb{Z} is definable over R and HTP is unsolvable over R .

(See Theorem 6.10.)

Remark 2.14. Note that in this paper we will have no assumptions on the nature of the totally real field besides the assumption on the existence of the elliptic curve satisfying the conditions above. Thus we will be able to consider a larger class of fields than in [25], [31], and [33].

Main Theorem E. Let K_∞ be a totally real possibly infinite algebraic extension of \mathbb{Q} normal over some number field K , with an odd rational prime $p > [K^{\text{Gal}} : \mathbb{Q}]$ of 0 degree index relative to K_∞ , and with a 0 degree index for 2. Let U_∞ be a finite extension of K_∞ such that there exists an elliptic curve \mathbf{E} defined over U_∞ with $\mathbf{E}(U_\infty)$ finitely generated and of a positive rank. Let GK_∞ be an extension of degree 2 over K_∞ .

- (1) GK_∞ contains a big ring where \mathbb{Z} is existentially definable and HTP is unsolvable.
- (2) \mathbb{Z} is definable and HTP is unsolvable over any small subring of GK_∞ .
- (3) If we assume additionally that the set of rational primes with 0 degree index with respect to K_∞ is infinite, then for every $\varepsilon > 0$ there exist a number field $K \subset K_\infty$ and a set $\mathcal{Z}_K \subset \mathcal{P}(K)$ of density (natural or Dirichlet) bigger than $1/2 - \varepsilon$ such that \mathbb{Z} is existentially definable and HTP is unsolvable in the integral closure of O_{K, \mathcal{Z}_K} in G_∞ .

(See Theorems 8.9 and 8.10.)

Main Theorem F. Let K_∞ be an algebraic extension of \mathbb{Q} such that there exists an elliptic curve \mathbf{E} defined over K_∞ with $\mathbf{E}(K_\infty)$ of rank 1 and finitely generated. Fix a Weierstrass equation for \mathbf{E} and a number field K containing all the coefficients of the Weierstrass equation and the coordinates of all the generators of $\mathbf{E}(K_\infty)$. Assume that K has two odd relative degree one primes \mathfrak{p} and \mathfrak{q} such that integrality is definable at \mathfrak{p} and \mathfrak{q} over K_∞ .

- (1) There exist a set \mathcal{W}_K of K -primes of natural density 1 such that over $O_{K_\infty, \mathcal{W}_{K_\infty}}$ there exists an infinite Diophantine set simultaneously discrete in all archimidean and non-archimidean topologies of K_∞ .
- (2) There exist a set \mathcal{W}_K of K -primes of natural density 1 such that over $O_{K_\infty, \mathcal{W}_{K_\infty}}$ there exists a Diophantine model of \mathbb{Z} and therefore HTP is not solvable over $O_{K_\infty, \mathcal{W}_{K_\infty}}$.

(See Theorem 9.10.)

3. BOUNDS AND THEIR USES.

We start with another notation set and some terminology.

Notation and Assumptions 3.1. We will use the following notation throughout the rest of the paper.

- Let T be any field and let $t \in T$. Then let $\mathfrak{d}_T(t) = \prod_{\mathfrak{p} \in \mathcal{P}(T)} \mathfrak{p}^{a(\mathfrak{p})}$, where the product is taken over all primes \mathfrak{p} of T such that $-a(\mathfrak{p}) = \text{ord}_{\mathfrak{p}} t < 0$. Further, let $\mathfrak{n}_T(t) = \mathfrak{d}_T(t^{-1})$.
- Let G/U be any number field extension. Let $\mathfrak{A} = \prod_{\mathfrak{p}_i \in \mathcal{P}(G)} \mathfrak{p}_i^{n_i}$ be an integral divisor of G such that \mathfrak{A} is equal to the factorization in G of some integral divisor of U . Then we will say that “ \mathfrak{A} can be considered as an integral divisor of U ”.
- Let T be a number field. Let $\mathfrak{A}, \mathfrak{B}$ be integral divisors of T such that for any $\mathfrak{p} \in \mathcal{P}(T)$ we have that $\text{ord}_{\mathfrak{p}} \mathfrak{A} \leq \text{ord}_{\mathfrak{p}} \mathfrak{B}$. Then we will say that “ \mathfrak{A} divides \mathfrak{B} in the semigroup of integral divisors of T ” or simply “ \mathfrak{A} divides \mathfrak{B} ”.
- Let T be a number field and let $\mathfrak{A}, \mathfrak{B}$ be divisors of T such that $\mathfrak{A} = \mathfrak{B}^2$. Then by $\sqrt{\mathfrak{A}}$ we will mean \mathfrak{B} .

Next we prove two technical lemmas dealing with bounds on valuations.

Lemma 3.2. *Let T be a number field, let $\mathcal{W}_T \subset \mathcal{P}(T)$. Let $x \in O_{T, \overline{\mathcal{W}_T}}, z \in O_{T, \mathcal{W}_T}, xz \neq 0$. Assume that $\mathfrak{n}_T(x)$ divides $\mathfrak{n}_T(z)$ in the semigroup of integral divisors of T . Let $X, Y, Z, W \in \mathbb{Z}_{>0}$ be such that $(X, Y) = 1, (Z, W) = 1, |\mathbf{N}_{T/\mathbb{Q}}(x)| = \frac{X}{Y}$, and $|\mathbf{N}_{T/\mathbb{Q}}(z)| = \frac{Z}{W}$. Then $\frac{Z}{X} \in \mathbb{Z}_{>0}$.*

Proof. Let $\mathfrak{Z}_1, \mathfrak{Z}_2, \mathfrak{W}, \mathfrak{X}, \mathfrak{Y}$ be integral divisors of T such that \mathfrak{Z}_1 and \mathfrak{X} are composed of the primes outside $\overline{\mathcal{W}_T}$, while $\mathfrak{Z}_2, \mathfrak{Y}, \mathfrak{W}$ are composed of primes in $\overline{\mathcal{W}_T}$, $\mathfrak{Z}_1, \mathfrak{Z}_2$, and \mathfrak{W} are pairwise relatively prime, \mathfrak{X} and \mathfrak{Y} are relatively prime, $\frac{\mathfrak{Z}_1 \mathfrak{Z}_2}{\mathfrak{W}}$ is a divisor of z , and $\frac{\mathfrak{X}}{\mathfrak{Y}}$ is a divisor of x . Since $\overline{\mathcal{W}_T}$ is closed under conjugation over \mathbb{Q} , we conclude that $\mathbf{N}_{T/\mathbb{Q}}(\mathfrak{X})$ and $\mathbf{N}_{T/\mathbb{Q}}(\mathfrak{Y})$ have no common factors as rational integers. Similarly, there are no rational primes occurring simultaneously in $\mathbf{N}_{T/\mathbb{Q}}(\mathfrak{Z}_1)$ and $\mathbf{N}_{T/\mathbb{Q}}(\mathfrak{W})$. So we can conclude that

$X = \mathbf{N}_{T/\mathbb{Q}}(\mathfrak{X})$ (as divisors of \mathbb{Q}), and $\mathbf{N}_{T/\mathbb{Q}}(\mathfrak{Z}_1)$ divides Z (as divisors of \mathbb{Q}). Further, by assumption, $\frac{\mathfrak{Z}_1}{\mathfrak{X}}$ is an integral divisor. Thus, $\frac{\mathbf{N}_{T/\mathbb{Q}}(\mathfrak{Z}_1)}{\mathbf{N}_{T/\mathbb{Q}}(\mathfrak{X})}$ is also an integral divisor. In other words, $\frac{Z}{X}$ is an integer. \square

Lemma 3.3. *Let T be a number field. Let \mathscr{W}_T be a set of primes of T . Let $x_1 \in O_{T, \overline{\mathscr{W}_T}}, x_1 \neq 0$ be such that x_1 does not have a positive order at any prime of $\overline{\mathscr{W}_T}$. Let $X, Y \in \mathbb{Z}_{>0}$ be such that $(X, Y) = 1, |\mathbf{N}_{T/\mathbb{Q}}(x_1)| = \frac{X}{Y}$. Let $x_2 \in O_{T, \overline{\mathscr{W}_T}}$ be a conjugate of x_1 over \mathbb{Q} . Then $Y^2 |\mathbf{N}_{T/\mathbb{Q}}(x_1 - x_2)| \in \mathbb{Z}_{>0}$.*

Proof. Let $\frac{\mathfrak{X}_1}{\mathfrak{Y}_1}, \frac{\mathfrak{X}_2}{\mathfrak{Y}_2}, \frac{\mathfrak{U}}{\mathfrak{V}}$ be the divisors of x_1, x_2 and $x_1 - x_2$ respectively. Observe that on the one hand, $\mathbf{N}_{T/\mathbb{Q}}(x_1) = \mathbf{N}_{T/\mathbb{Q}}(x_2) = \frac{X}{Y}$ and, using the same argument as in the proof of Lemma 3.2, we have that $\mathbf{N}_{T/\mathbb{Q}}(\mathfrak{Y}_1) = \mathbf{N}_{T/\mathbb{Q}}(\mathfrak{Y}_2) = Y$. On the other hand, \mathfrak{V} divides $\mathfrak{Y}_1 \mathfrak{Y}_2$ in the semigroup of integral divisors and therefore, $\mathbf{N}_{T/\mathbb{Q}}(\mathfrak{V})$ divides Y^2 in the semigroup of integral divisors of \mathbb{Q} . Further, if we let $\mathbf{N}_{T/\mathbb{Q}}(x_1 - x_2) = \frac{A}{B}$, with A and B being relatively prime integers, then B divides $\mathbf{N}_{T/\mathbb{Q}}(\mathfrak{V})$ in the integral divisor semigroup of \mathbb{Q} . Thus, B divides Y^2 in \mathbb{Z} . \square

Now consider the following use of bounds:

Proposition 3.4. *Let U be a number field. Let $\mathscr{W}_U \subset \mathscr{P}(U)$. Let p be a rational prime such that no factor of p is in \mathscr{W}_U . Let x, z be elements of the algebraic closure of U and assume that for any prime \mathfrak{q} of $U(x, z)$ lying above a prime of $\overline{\mathscr{W}_U}$ we have that $\text{ord}_{\mathfrak{q}} x \leq 0$ and $\text{ord}_{\mathfrak{q}} z \leq 0$. Let T be the Galois closure of $U(x, z)$. Let $t \in O_{U, \mathscr{W}_U}$. Assume also that $\mathbf{n}_T(z)$ can be considered as a divisor of U . Finally assume that the following equations and conditions are satisfied over O_{T, \mathscr{W}_T} , where $\text{id} = \sigma_1, \dots, \sigma_{[T:\mathbb{Q}]}$ are all the distinct embeddings of T into \mathbb{C} .*

$$(3.1) \quad |\sigma_i(x)| \leq |\sigma_i(z)|, i = 1, \dots, [T:\mathbb{Q}],$$

$$(3.2) \quad |\sigma_i(x)| \geq 1, i = 1, \dots, [T:\mathbb{Q}],$$

$$(3.3) \quad |\sigma_i(z)| > 1, i = 1, \dots, [T:\mathbb{Q}],$$

$$(3.4) \quad z \equiv 0 \pmod{x \text{ in } O_{T, \mathscr{W}_T}},$$

$$(3.5) \quad x \equiv t \pmod{pz^4 \text{ in } O_{T, \mathscr{W}_T}}.$$

Then $x \in O_{U, \mathscr{W}_U}$.

Proof. Using notation of Lemma 3.2, let $|\mathbf{N}_{T/\mathbb{Q}}(x)| = \frac{X}{Y}$, where (X, Y) are relatively prime positive integers, and let $|\mathbf{N}_{T/\mathbb{Q}}(z)| = \frac{Z}{W}$, where $Z, W \in \mathbb{Z}_{>0}$ and $(Z, W) = 1$ in \mathbb{Z} . Then by Lemma 3.2 we have that X divides Z in \mathbb{Z} and therefore $1 \leq X \leq Z$. Further, from equation (3.2), we also have that

$$(3.6) \quad Y \leq X \leq Z.$$

Let $\mathfrak{Z} = \mathbf{n}_T(z)$. From (3.5) we have that $p\mathfrak{Z}^4$ divide $\mathbf{n}_T(x - t)$. Now, assume that \hat{x} is a conjugate of x over U . Then $p\mathfrak{Z}^4$ divides $\mathbf{n}_T(x - \hat{x})$ in the semigroup of integral divisors of T . Let

$$(3.7) \quad |\mathbf{N}_{T/\mathbb{Q}}(x - \hat{x})| = \frac{A}{B},$$

where A, B are relatively prime positive integers. Then on the one hand, by Lemma 3.2 again, we have that either $x = \hat{x}$ or $p^{[T:\mathbb{Q}]}Z^4$ divides A and therefore

$$(3.8) \quad p^{[T:\mathbb{Q}]}Z^4 \leq A.$$

On the other hand, from equation (3.1) we have that the absolute value of any conjugate of $x - \hat{x}$ over \mathbb{Q} is less than 2 times the absolute value of the corresponding conjugate of z . Thus,

$$(3.9) \quad |\mathbf{N}_{T/\mathbb{Q}}(x - \hat{x})| \leq 2^{[T:\mathbb{Q}]} |\mathbf{N}_{T/\mathbb{Q}}(z)|.$$

Using equation (3.7) we can now write

$$(3.10) \quad \frac{A}{B} \leq 2^{[T:\mathbb{Q}]} |\mathbf{N}_{T/\mathbb{Q}}(z)|$$

and so

$$(3.11) \quad A \leq 2^{[T:\mathbb{Q}]} B |\mathbf{N}_{T/\mathbb{Q}}(z)|.$$

Thus, combining (3.11), (3.8), (3.6) and using Lemma 3.3 we get

$$(3.12) \quad p^{[T:\mathbb{Q}]} Z^4 \leq 2^{[T:\mathbb{Q}]} B |\mathbf{N}_{T/\mathbb{Q}}(z)| = 2^{[T:\mathbb{Q}]} B \frac{Z}{W} \leq 2^{[T:\mathbb{Q}]} Y^2 \frac{Z}{W} \leq 2^{[T:\mathbb{Q}]} Z^3.$$

Since $p \geq 2$ and from equation (3.2) we know that $Z > 1$, the last inequality cannot be true. Thus, $x = \hat{x}$. Since \hat{x} was an arbitrary conjugate of x over U , we must conclude that $x \in U$. \square

The bounds also come in the following lemma which we will use below. It is a slight modification of Lemma 5.1 of [31].

Lemma 3.5. *Let T/U be an extension of number fields. Let $x \in T$ and let $\mathfrak{T} = \mathbf{n}_T(x)$. Let \mathfrak{A} be an integral divisor of U such that \mathfrak{T}^2 divides \mathfrak{A} in the semigroup of the integral divisors of T . Let $t \in U$ be such that \mathfrak{A} divides $\mathfrak{M} = \mathbf{n}_T(x - t)$ in the semigroup of integral divisors of T . Then \mathfrak{T} can be considered as a divisor of U .*

Proof. We will show that for all $\mathfrak{p} \in \mathcal{P}(T)$, such that $\text{ord}_{\mathfrak{p}} x > 0$ we have that $\text{ord}_{\mathfrak{p}} x = \text{ord}_{\mathfrak{p}} t$, and for any \mathfrak{q} conjugate to \mathfrak{p} over U we also have that $\text{ord}_{\mathfrak{q}} x = \text{ord}_{\mathfrak{q}} t > 0$. Indeed, let \mathfrak{p} be a prime of T such that $\text{ord}_{\mathfrak{p}} x > 0$. Then given our assumptions on \mathfrak{A} we have that $\text{ord}_{\mathfrak{p}}(x - t) > \text{ord}_{\mathfrak{p}} x$. The only way this can happen is for $\text{ord}_{\mathfrak{p}} x = \text{ord}_{\mathfrak{p}} t > 0$. Next note that if \mathfrak{q} is a conjugate of \mathfrak{p} over U , then $\text{ord}_{\mathfrak{q}} \mathfrak{A} > 0$ implying that $\text{ord}_{\mathfrak{q}}(x - t) > 0$ and since $t \in T$, we also have that $\text{ord}_{\mathfrak{q}} t > 0$. Thus, $\text{ord}_{\mathfrak{q}} x > 0$ and as above $\text{ord}_{\mathfrak{q}} x = \text{ord}_{\mathfrak{q}} t > 0$. Thus, \mathfrak{T} can be viewed as a divisor of U . \square

4. PROPERTIES OF ELLIPTIC CURVES

In this section we go over some properties of elliptic curves which will allow us to make sure we can satisfy equivalencies of the form (3.4) and (3.5).

Notation 4.1. We start with a notation set to be used below.

- Let U be a number field.
- Let E denote an elliptic curve defined over U – i.e. a non-singular cubic curve whose affine part is given by a fixed Weierstrass equation with coefficients in O_U . (See III.1 of [35].)
- For any field T and any $m \in \mathbb{Z}_{\geq 0}$ let $E(T)[m]$ be the group of m -torsion points of $E(T)$. By “0-torsion” we mean the identity of E .
- If $Q \in E(U)$ is any point, then $(x(Q), y(Q))$ will denote the affine coordinates of Q given by the Weierstrass equation above.
- Let P be a fixed point of infinite order.
- Let U_{∞}/U be an infinite abelian Galois extension.
- Assume $\text{rank}(E(U_{\infty})) = \text{rank}(E(U))$.

Lemma 4.2. *If $I \subset O_U$ is a nonzero ideal. Then there exists a non-zero multiple $[l]P$ of P such that $I \mid \mathfrak{d}(x([l]P))$.*

Proof. This lemma follows immediately from Lemma 10 of [16] even though we no longer assume that the curve is of rank 1. The proof is unaffected by this change. \square

Lemma 4.3. *There exists a positive integer r such that for any positive integers l, m ,*

$$\mathfrak{d}_U(x([lr]P)) \mid \mathbf{n}_U\left(\frac{x[lr](P)}{x([mlr]P)} - m^2\right)^2.$$

Proof. Let r be a positive integer defined in Lemma 8 of [16]. Then the statement above follows immediately from Lemma 11 of [16]. The proof is again unaffected by the fact that we no longer assume E to be of rank 1. \square

Lemma 4.4. *Let r be as in Lemma 4.3. Let $Q', Q \in [r]\mathbf{E}(U) \setminus \{O\}$, $Q' = [k]Q$. Then $\mathfrak{d}_U(x(Q))$ divides $\mathfrak{d}_U(x(Q'))$ in the semigroup of integral divisors of U .*

Proof. See Lemma 9 of [16]. □

Lemma 4.5. *Let Q, Q' be as in Lemma 4.4. Then $\mathfrak{d}_U(x(Q))$ and $\mathfrak{d}_U\left(\frac{x(Q)}{x(Q')}\right)$ do not have any common factors.*

Proof. By Lemma 4.4 we know that $\frac{\mathfrak{d}_U(x(Q'))}{\mathfrak{d}_U(x(Q))} = \mathfrak{A}$ is an integral divisor. Next we note that the divisor of $\frac{x(Q)}{x(Q')}$ is of the form

$$\frac{\mathfrak{n}_U(x(Q))\mathfrak{d}_U(x(Q'))}{\mathfrak{d}_U(x(Q))\mathfrak{n}_U(x(Q'))} = \frac{\mathfrak{A}\mathfrak{n}_U(x(Q))}{\mathfrak{n}_U(x(Q'))}$$

so that $\mathfrak{d}_U\left(\frac{x(Q)}{x(Q')}\right)$ divides $\mathfrak{n}_U(x(Q'))$ in the group of integral divisors of U . Now $\mathfrak{n}_U(x(Q'))$ has no common factors with $\mathfrak{d}_U(x(Q'))$ and thus with $\mathfrak{d}_U(x(Q))$. Consequently, $\mathfrak{d}_U\left(\frac{x(Q)}{x(Q')}\right)$ has no common factors with $\mathfrak{d}_U(x(Q))$ □

The last lemma of this section follows from the chosen form of the Weierstrass equation.

Lemma 4.6. *$\mathfrak{d}_U(x(Q))$ is a square of an integral divisor of U .*

The next two propositions will provide foundations for a construction of examples of elliptic curves with finitely generated groups in some infinite extensions. We first state a theorem which is a special case of Theorem 12 from [34]. For our special case below we can set the parameter $[F(nP) : F]$ to 1.

Theorem 4.7. *Let F/\mathbb{Q} be a number field, let \mathbf{E}/F be an elliptic curve that does not have complex multiplication. Then there is an integer $k = k(\mathbf{E}/F)$ so that for any point $P \in \mathbf{E}(\bar{\mathbb{Q}})$, where $\bar{\mathbb{Q}}$ is the algebraic closure of \mathbb{Q} , with $F(P)/F$ abelian we have that $[F(P) : F]$ divides $k[F(nP) : F]$ for all n .*

We now use the theorem to prove that $\mathbf{E}(U_\infty)$ is finitely generated. The proof of the proposition was suggested to the author by Karl Rubin.

Proposition 4.8. *$\mathbf{E}(U_\infty)$ is finitely generated.*

Proof. Let k be a positive integer defined in Theorem 4.7. Since $\text{rank}(\mathbf{E}(U_\infty)) = \text{rank}(\mathbf{E}(U))$, for any $Q \in \mathbf{E}(U_\infty)$ for some $m \in \mathbb{Z}_{>0}$ we have that $[m]Q \in \mathbf{E}(U)$. Further, since U_∞/U is abelian, we also have that $U(Q)/U$ is abelian. Thus, m divides k and $\mathbf{E}(U_\infty)$ is finitely generated. □

5. DIOPHANTINE DEFINITIONS OF RATIONAL INTEGERS FOR THE TOTALLY REAL CASE.

In this section we construct Diophantine definitions of \mathbb{Z} and *some* rings of rational \mathcal{S} -integers with finite \mathcal{S} which we also called the small rings.

Notation and Assumptions 5.1. We add the following notation and assumptions to our notation and assumption list.

- Let K be a totally real number field.
- Let K_∞ be a possibly infinite totally real extension of K .
- Let F be a finite extension of K such that $F \cap K_\infty = K$. (F can be equal to K .)
- Let \mathbf{E} denote an elliptic curve defined over F with $\text{rank} \mathbf{E}(F) > 0$ and $i = [\mathbf{E}(FK_\infty) : \mathbf{E}(F)] < \infty$.
- Let O denote the identity element of the Mordell-Weil group of \mathbf{E} .

We will separate our Diophantine definition into two parts.

Lemma 5.2. *Under assumptions in 5.1 there exists a set \mathbf{A} contained in O_{FK_∞} and Diophantine over O_{FK_∞} , such that if $x \in \mathbf{A}$ then $\mathfrak{n}_{F(x)}(x)$ can be considered as a divisor of F . Further, if x is a square of a rational integer, then $x \in \mathbf{A}$, and all the equations comprising the Diophantine definition of \mathbf{A} can be satisfied with variables (except for the variables representing the points on \mathbf{E}) ranging over O_F .*

Proof. Consider the following equations, where $x, u_Q, v_Q, w, Z, W, A, a, b \in O_{FK_\infty}, x(Q), x(S) \in FK_\infty$.

$$(5.1) \quad S, Q \in [i]E(FK_\infty) \setminus \{O\},$$

$$(5.2) \quad x(Q) = \frac{u_Q}{v_Q},$$

$$(5.3) \quad Xb + Yv_Q = 1$$

$$(5.4) \quad Zx + Wu_Q = 1$$

$$(5.5) \quad \frac{x(Q)}{x(S)} = \frac{a}{b},$$

$$(5.6) \quad u_Q(xb - a)^2 = v_Qw,$$

$$(5.7) \quad v_Q = x^4A.$$

Indeed suppose that equations (5.1)–(5.7) are satisfied with all the variables ranging over the sets described above. Let $M = K(x)$. From equation (5.1) we know that $x(Q) \in F$. Since $x(Q) \in F$, by Lemma 4.6, we can conclude that $\mathfrak{d}_{FM}(x(Q))$ can be viewed as a second power of a divisor of F . Note that $\mathfrak{n}_{FM}(v_Q) = \mathfrak{d}_{FM}(x(Q))\mathfrak{W}$, where \mathfrak{W} is an integral divisor of FM and \mathfrak{W} divides $\mathfrak{n}_{FM}(u_Q)$ in the integral divisor semigroup of FM . Since $(u_Q, x) = 1$ from (5.4), we must conclude that $\mathfrak{n}_{FM}(x^4)$ divides $\mathfrak{d}_{FM}(x(Q))$ in the integral divisor semigroup of FM . From (5.6) we see that $\mathfrak{n}_{FM}\left(\frac{v_Q}{u_Q}\right)$, and therefore $\mathfrak{d}_{FM}(x(Q))$, divide $\mathfrak{n}_{FM}(xb - a)^2$. Since b and v_Q are relatively prime by (5.3), we deduce that $\sqrt{\mathfrak{d}_{FM}(x(Q))}$ also divides $\mathfrak{n}_{FM}\left(x - \frac{a}{b}\right)$. Next note that $\frac{a}{b} \in F$ and by Lemma 3.5 we have the desired conclusion.

Suppose now that $x = m^2$ where $m \in \mathbb{Z}_{>0}$. Let $Q \in [i]E(FK_\infty)$ be of infinite order and such that m^4 divides $\mathfrak{d}_F(x(Q))$. Such an Q exists by Lemma 4.2. Let $S = [m]Q$. By Lemma 4.5 we have that $\mathfrak{d}_{FM}(x(Q))$ is relatively prime to $\mathfrak{d}_{FM}\left(\frac{x(Q)}{x(S)}\right)$. Thus by Lemma 11.1 we can write $x(Q) = \frac{u_Q}{v_Q}, \frac{x(Q)}{x(S)} = \frac{a}{b}$, where $u_Q, v_Q, a, b \in O_F, (v_Q, b) = 1, (\mathfrak{n}_F(u_Q), \mathfrak{d}_F(x(Q))) = 1$. Therefore, since $\mathfrak{n}_F(x)$ divides $\mathfrak{d}_F(x(Q))$, we also have that $(x, u_Q) = 1$. Further by Lemma 4.3, we also have $\mathfrak{d}_F(x(Q))$ divides $\mathfrak{n}_F\left(\frac{x(Q)}{x(S)} - m^2\right)^2$ as integral divisors of F . As above $\mathfrak{n}_F(v_Q) = \mathfrak{d}_F(x(Q))\mathfrak{W}$, where \mathfrak{W} is an integral divisor dividing $\mathfrak{n}_F(u_Q)$. Therefore $\mathfrak{n}_F(v_Q)$ divides $\mathfrak{n}_F(u_Q)\mathfrak{n}_F\left(\frac{x(Q)}{x(S)} - m^2\right)^2$. Thus all the equations above can be satisfied.

Finally we note that all the equations above can be rewritten so that the variables range over O_{FK_∞} only. \square

We now proceed to the second part Diophantine definition.

Proposition 5.3. *Consider the following equations and conditions, where $x, z \in O_{K_\infty}; x(Q), x(P_j) \in FK_\infty; u_Q, v_Q, y_j, a_j, b_j, X_j, Y_j, c_j, d_j, U_j, V_j \in O_{FK_\infty}; j = 0, 1, 2$.*

$$(5.8) \quad z \in \mathbf{A},$$

$$(5.9) \quad x_j = (x + j)^2 \in \mathbf{A}, j = 0, 1, 2$$

$$(5.10) \quad \sigma(x_j) \geq 1, j = 0, 1, 2$$

for all σ , embeddings of K_∞ into \mathbb{R} ,

$$(5.11) \quad Q, P_0, P_1, P_2 \in [i]E(FK_\infty) \setminus \{O\},$$

$$(5.12) \quad \sigma(z) > \max\{\sigma(x_0), \sigma(x_1), \sigma(x_2)\}$$

for all σ , embeddings of K_∞ into \mathbb{R} ,

$$(5.13) \quad z_j = x_j z, j = 0, 1, 2$$

$$(5.14) \quad x(Q) = \frac{u_Q}{v_Q},$$

$$(5.15) \quad X_j v_Q + Y_j b_j = 1$$

$$(5.16) \quad U_j z_j + V_j u_Q = 1$$

$$(5.17) \quad \frac{a_j}{b_j} = \frac{x(Q)}{x(P_j)}, j = 0, 1, 2$$

$$(5.18) \quad v_Q = p^2 z_j^8 y_j,$$

$$(5.19) \quad u_Q(x_j b_j - a_j)^2 = c_j v_Q, j = 0, 1, 2$$

We claim that if these equations are satisfied with variables in the sets as indicated above, then $x \in O_K$. Conversely, if $x \in \mathbb{Z}_{>0}$ then all the equations can be satisfied with $z, y, y_j, x_j \in O_K; x(Q), x(P_j) \in F; a, b, u_j \in O_{FK}; j = 0, 1, 2$.

Proof. Let M be the Galois closure of $K(x, z)$ over \mathbb{Q} . From equation (5.9) we conclude that $x_j \in M \subset FM, j = 0, 1, 2$. Observe also that from (5.8) and (5.9) we have that z and x_j are elements of \mathbf{A} , and thus by definition of \mathbf{A} , we have that $\mathfrak{n}_{FM}(z_j) = \mathfrak{n}_{FM}(x_j z)$ can be considered as a divisor of F . Further, from (5.10) and (5.12) we have that

$$(5.20) \quad 1 \leq \sigma(x_j) < \sigma(z_j)$$

for any embedding $\sigma : FM \rightarrow \mathbb{C}$. Next using the fact that b_j and v_Q are relatively prime by equation (5.15), as in Lemma 5.2 we conclude that $\mathfrak{d}_{FM}\left(\frac{x(Q)}{x(P_j)}\right)$ divides $\mathfrak{n}_{FM}\left(x_j - \frac{a_j}{b_j}\right)^2$ for $j = 0, 1, 2$ in the integral divisor semigroup of FM . Next, again as in Lemma 5.2, since $\mathfrak{n}_{FM}(p^2 z_j^8)$ divides $\mathfrak{d}_{FM}(x(Q))$ in the integral divisor semigroup of FM by equation (5.18) and equation (5.16), we also have that $\mathfrak{n}_{FM}(p z_j^4)$ divides $\mathfrak{n}_{FM}\left(x_j - \frac{a_j}{b_j}\right)$ for $j = 0, 1, 2$. Now by Proposition 3.4, we can conclude that $x_j \in F$. But $x_j \in M$ and $M \cap F = K$. Thus for all $j = 0, 1, 2$ we have that $x_j \in K$. Now by Lemma 5.1 of [26], we can conclude that $x \in K$.

Suppose now that $x \in \mathbb{Z}_{>0}$. Then x_j is a non-zero square of a rational integer. Next choose z to be a square of a rational integer satisfying (5.12). From this point on the argument proceeds in the same fashion as in Lemma 5.2. \square

The last lemma is all we need for the proof of the following theorem.

Theorem 5.4. *Let K be a totally real field. Let K_∞ a totally real possibly infinite algebraic extension of K . Let F be a finite extension of K such that for some elliptic curve E defined over F and of a positive rank over F we have that $[E(FK_\infty) : E(F)] < \infty$ and $K_\infty \cap F = K$. Then O_K and \mathbb{Z} have a Diophantine definition over O_{K_∞} and Hilbert's Tenth Problem is not solvable over O_{K_∞} .*

We now state a corollary whose proof follows from our definition of definability of integrality at a finite set of primes in infinite algebraic extensions.

Corollary 5.5. *Let $\mathcal{C}_K \subset \mathcal{P}(K)$ be a set of primes of K such that integrality is definable at primes of \mathcal{C}_K in K_∞ . Then $O_{K, \mathcal{C}_K}, O_K$ and \mathbb{Z} are existentially definable over $O_{K_\infty, \mathcal{C}_{K_\infty}}$ and therefore HTP is not solvable over $O_{K_\infty, \mathcal{C}_{K_\infty}}$.*

Theorem 5.4 and Corollary can also be stated in a different way avoiding reference to any number fields. (See Main Theorem A.)

Theorem 5.6. *Let K_∞ be a totally real possibly infinite algebraic extension of \mathbb{Q} . Let U_∞ be a finite extension of K_∞ such that there exists an elliptic curve \mathbf{E} defined over U_∞ with $\mathbf{E}(U_\infty)$ finitely generated and of a positive rank. Then \mathbb{Z} is existentially definable and HTP is unsolvable over the ring of integers of K_∞ . Further, \mathbb{Z} is existentially definable and HTP is unsolvable over any small subring of K_∞ where integrality is definable at all the primes allowed in the denominator of the divisors of elements of the ring.*

6. DIOPHANTINE DEFINITIONS OF SOME BIG AND ARBITRARY SMALL SUBRINGS OF RATIONAL NUMBERS FOR THE TOTALLY REAL CASE.

In this section we will consider large rings and arbitrary small rings. However in order to be able to manage large sets of primes in the denominator it is necessary to make additional assumptions on the nature of the infinite extension K_∞ . These extra assumptions are listed below.

Notation and Assumptions 6.1. In what follows we add the following to the list of notation and assumptions.

- K_∞ is normal over K .
- Let E be a number field satisfying the following conditions:
 - $n_E = [E : \mathbb{Q}] = [EK : K]$.
 - For any number field $M \subset K_\infty$ and such that $K \subset M$ we have that $([M : K], n_E) = 1$.
- Let $\mu_E \in O_E$ be a generator of E over \mathbb{Q} . Assume also that μ_E is an integral unit. Let $R(T) \in \mathbb{Z}[T]$ be the monic irreducible polynomial of an integral generator μ_E of E over \mathbb{Q} .
- Let $\mathcal{V}_K \subset \mathcal{P}(K)$ be a set of primes of K without relative degree 1 factors in E .
- Let \mathcal{S}_K be a finite set of primes of K .
- Let $\mathcal{W}_K = \mathcal{V}_K \cup \mathcal{S}_K$.
- Let \mathcal{E}_K consist of all the primes \mathfrak{p}_K of \mathcal{W}_K such that either \mathfrak{p}_K divides the discriminant of $R(T)$ or \mathfrak{p}_K has a relative degree 1 factor in the extension EK/K .
- For any $C > 0$, let $A(C) \geq 2$ be an integer such that for any real $t > A(C)$ we have that $R(t) > C$.
- Let $N_0 = 0, \dots, N_{2n_E}$ be positive integers selected so that the set of polynomials $\{R(A(1) + x + N_j)^2\}$ is linearly independent. Such a set of positive integers exists by Lemma 12.1 of [33].)
- Let p be a rational prime without any factors in \mathcal{W}_K .
- For any number field U , any set $\mathcal{D}_U \subset \mathcal{P}(U)$ and any $x \in U$ let

$$\mathfrak{n}_{U, \mathcal{D}_U}(x) = \prod_{\mathfrak{p} \in \mathcal{P}(U) \setminus \mathcal{D}_U, \text{ord}_{\mathfrak{p}} x > 0} \mathfrak{p}^{\text{ord}_{\mathfrak{p}} x}$$

We start with some observations concerning our prime sets.

Lemma 6.2. (1) \mathcal{E}_K is a finite set of primes.
 (2) All the primes of \mathcal{E}_K are K_∞ -boundable.

Proof. (1) Only finitely many can divide the discriminant of $R(T)$.

- (2) By assumption the extension K_∞/K satisfies the requirement of Corollary 2.4. Thus, any finite set of primes of K is K_∞ -boundable. □

Next we note that from our assumptions on the degree of subextensions of K_∞ and Lemma 11.2 we can obtain the following lemma.

Lemma 6.3. *Let $M \subset K_\infty$ be a number field containing K . Let \mathfrak{p}_M be a prime lying above a prime of K without relative degree one factors in the extension EK/K . Then \mathfrak{p}_M does not have a relative degree one factor in the extension EM/M .*

We now proceed to the big ring versions of Lemma 5.2 and Proposition 5.3.

Lemma 6.4. *The exist a set \mathbf{A} contained in $O_{FK_\infty, \mathcal{W}_{K_\infty}}$ and Diophantine over $O_{FK_\infty, \mathcal{W}_{K_\infty}}$, such that if $\text{ord}_{\mathfrak{p}} x \leq 0$ for all \mathfrak{p} in $F(x)$ lying above primes in $\overline{\mathcal{W}}_F$, and $x \in \mathbf{A}$, then $\mathfrak{n}_{F(x)}(x)$ can be considered as a*

divisor of F (composed solely of factors of F -primes outside $\overline{\mathcal{W}}_F$). Further, if x is a square of a rational integer then $x \in \mathbf{A}$ and all the equations comprising the Diophantine definition can be satisfied with variables ranging over O_{F, \mathcal{W}_F} .

Proof. Consider the following equations, where $x, y \in O_{FK_\infty, \mathcal{W}_{FK_\infty}}, u_Q, v_Q, w, A, B, C \in O_{FK_\infty, \mathcal{W}_{FK_\infty}}, x(Q), x(R) \in FK_\infty$ and $\text{ord}_{\mathfrak{p}} x \leq 0$ for all \mathfrak{p} in $F(x)$ lying above primes in $\overline{\mathcal{W}}_F$.

$$(6.21) \quad S, Q, \in [i]\mathbf{E}(FK_\infty) \setminus \{O\},$$

$$(6.22) \quad x(Q) = \frac{u_Q}{v_Q}, v_Q \neq 0,$$

$$(6.23) \quad Xb + Yv_Q = 1$$

$$(6.24) \quad \frac{x(Q)}{x(S)} = \frac{a}{b}$$

$$(6.25) \quad Zx + Wu_Q = 1$$

$$(6.26) \quad u_Q(bx - a)^2 = v_Qw,$$

$$(6.27) \quad v_Q = x^4A.$$

We claim that if for some $x \in O_{FK_\infty, \mathcal{W}_{FK_\infty}}$ these equations are satisfied with all the variable as indicated above, then x satisfies the requirements for the membership in \mathbf{A} as described in the statement of the lemma, and if x is a square of an integer, then all the equations can be satisfied with all the variables ranging over O_{F, \mathcal{W}_F} .

Indeed suppose that equations (6.21)–(6.27) are satisfied with all the variables ranging over the sets described above. Let $M = K(x)$. Then by assumption we have that for all $\mathfrak{p} \in \overline{\mathcal{W}}_{FM}$ it is the case that $\text{ord}_{\mathfrak{p}} x \leq 0$. Next let $\mathfrak{d}_{FM}(x(Q)) = \mathfrak{N}_1\mathfrak{N}_2$, where $\mathfrak{N}_1, \mathfrak{N}_2$ are integral divisors of FM , all the primes occurring in \mathfrak{N}_1 are outside $\overline{\mathcal{W}}_{FM}$ and all the primes occurring in \mathfrak{N}_2 are in $\overline{\mathcal{W}}_{FM}$. Since $x(Q) \in F$ and $\overline{\mathcal{W}}_{FM}$ is, by definition, closed under conjugation over F , by Lemma 4.6, we can conclude that $\mathfrak{N}_1, \mathfrak{N}_2$ can be both viewed as second powers of divisors of F . Next write

$$(6.28) \quad \mathfrak{n}_{FM}(v_Q) = \mathfrak{N}_1\mathfrak{A}\mathfrak{B}, \mathfrak{n}_{FM}(u_Q) = \mathfrak{C}\mathfrak{A}\mathfrak{D},$$

where $\mathfrak{N}_1, \mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \mathfrak{D}$ are integral divisors of FM , $\mathfrak{N}_1, \mathfrak{A}, \mathfrak{B}$ are pairwise relatively prime, $\mathfrak{C}, \mathfrak{A}, \mathfrak{D}$ are pairwise relatively prime, $\mathfrak{C}, \mathfrak{A}$ are composed of primes outside $\overline{\mathcal{W}}_{FM}$ only, while $\mathfrak{B}, \mathfrak{D}$ are composed of primes in $\overline{\mathcal{W}}_{FM}$. From equation (6.25) we can conclude that $(\mathfrak{n}_{FM}(x), \mathfrak{A}) = 1$, and since x does not have a positive order at any prime of $\overline{\mathcal{W}}_{FM}$, we can conclude from equation (6.27) that $\mathfrak{n}_{FM}(x)$ divides \mathfrak{N}_1 in the integral divisor semigroup of FM . From (6.23) we know that $\mathfrak{n}_{FM}(b)$ is relatively prime to \mathfrak{N}_1 and we have already established that \mathfrak{N}_1 is relatively prime to $\mathfrak{n}_{FM}(u_Q)$. So if we let $\mathfrak{M} = \mathfrak{n}_{FM}\left(x - \frac{a}{b}\right)$. Then from (6.26) we conclude that \mathfrak{N}_1 divides \mathfrak{M} in the semigroup of integral divisors of FM . Therefore, by Lemma 3.5 we have the desired conclusion.

Suppose now that $x = m^2$ where $m \in \mathbb{Z}_{>0}$. Then we can again proceed as in Lemma 5.2.

Finally we note that all the equations above can be rewritten so that the variables range over O_{F, \mathcal{W}_F} only. \square

We now proceed to the part two of the big ring Diophantine definition.

Proposition 6.5. *Consider the following equations and conditions, where $x, z, z_0, x_j \in O_{K_\infty, \mathscr{W}_{K_\infty}}; x(Q), x(P_j) \in FK_\infty; a_j, b_j, c_j, X_j, Y_j, Z_j, W_j, w_j \in O_{FK_\infty, \mathscr{W}_{FK_\infty}}; j = 0, \dots, 2n_E$.*

$$(6.29) \quad z = R(z_0) \in \mathbf{A},$$

$$(6.30) \quad x_j = (R(A(1) + x + N_j))^2 \in \mathbf{A}, j = 0, \dots, 2n_E,$$

$$(6.31) \quad \sigma(x_j) \geq 1$$

for all $\sigma : K_\infty \rightarrow \mathbb{R}$,

$$(6.32) \quad Q, P_1, \dots, P_{2n_E} \in [i]\mathbf{E}(FK_\infty) \setminus \{O\},$$

$$(6.33) \quad \sigma(z) \geq \max\{\sigma(x_1), \dots, \sigma(x_{2n_E})\}$$

for all σ , embeddings of K_∞ into \mathbb{R} ,

$$(6.34) \quad z_j = x_j z$$

$$(6.35) \quad x(Q) = \frac{u_Q}{v_Q},$$

$$(6.36) \quad X_j b_j + Y_j v_Q = 1$$

$$(6.37) \quad \frac{x(Q)}{x(P_j)} = \frac{a_j}{b_j}$$

$$(6.38) \quad Z_j z_j + W_j u_Q = 1$$

$$(6.39) \quad v_Q = p^2 z_j^8 w_j$$

$$(6.40) \quad u_Q(b_j x_j - a_j)^2 = v_Q c_j.$$

We claim that if these equations are satisfied with variables in the sets as indicated above, then $x \in O_{K, \mathscr{W}_K}$. Conversely, if $x \in \mathbb{Z}_{>0}$ then all the equations can be satisfied with $z_0, x \in O_{K, \mathscr{W}_K}; x(Q), x(P_j) \in F; a_j, b_j, c_j, w_j, X_j, Y_j, Z_j, W_j \in O_{F, \mathscr{W}_F}; j = 0, \dots, 2n_E$.

Proof. Let M be the Galois closure of $K(x, z_0)$ over \mathbb{Q} . Next from equation (6.30) we conclude that $x_j \in M \subset MF, j = 0, \dots, 2n_E$ and by Lemma 2.8,

$$(6.41) \quad \forall \mathfrak{p} \in \overline{\mathscr{W}}_M : \text{ord}_{\mathfrak{p}} x_j \leq 0.$$

Similarly, we have from (6.29) that

$$(6.42) \quad \forall \mathfrak{p} \in \overline{\mathscr{W}}_M : \text{ord}_{\mathfrak{p}} z \leq 0.$$

Observe also that from (6.30) and (6.29) we deduce that z and x_j are elements of \mathbf{A} , and thus by definition of \mathbf{A} , we have that $\mathfrak{n}_{MF}(z_j) = \mathfrak{n}_{MF}(x_j z)$ can be considered as a divisor of F . Additionally from (6.41) and (6.42) we know that all the primes occurring in $\mathfrak{n}_{MF}(z_j)$ are outside $\overline{\mathscr{W}}_{MF}$. Further from (6.31) and (6.33) we now have that

$$(6.43) \quad 1 \leq \sigma(x_j) \leq \sigma(z_j)$$

for any embedding $\sigma : MF \rightarrow \mathbb{C}$. Next using equations (6.39) and (6.38), by an argument analogous to the one used in Lemma 5.2, we observe that $\mathfrak{n}_{MF}(p z_j^4)$ divides $\mathfrak{n}_{MF}(x_j - \frac{a_j}{b_j})$ for all $j = 0, \dots, 2n_E$.

Now by Proposition 3.4, we can conclude that $x_j \in F$. But $x_j \in M$ and $M \cap F = K$. Thus for all $j = 0, \dots, 2n_E$ we have that $x_j \in K$. Further, by our assumption on N_0, \dots, N_{2n_E} and by Lemma 5.1 of [26], we can conclude that $x \in K$.

Suppose now that $x \in \mathbb{Z}_{>0}$. Then x_j is a non-zero square of a rational integer. From this point on the argument proceeds in the same fashion as in Lemma 5.2. \square

We are now ready for the main theorem.

Theorem 6.6. *There exists a polynomial equation $P(x, \bar{t}) \in O_K[x, \bar{t}]$ such that the following statements are true.*

- (1) *For any $x \in O_{K_\infty, \mathcal{W}_{K_\infty}}$, if $P(x, \bar{t}) = 0$ for some $\bar{t} = (t_1, \dots, t_m)$ with $t_i \in O_{K_\infty, \mathcal{W}_{K_\infty}}$, then $x \in O_{K, \mathcal{W}_K}$.*
- (2) *If $x \in \mathbb{Z}$ there exists $\bar{t} = (t_1, \dots, t_m)$ with $t_i \in O_{K, \mathcal{W}_K}$ such that $P(x, \bar{t}) = 0$*
- (3) *$O_{K_\infty, \mathcal{W}_{K_\infty}} \cap K = O_{K, \mathcal{W}_K}$ has a Diophantine definition over $O_{K_\infty, \mathcal{W}_{K_\infty}}$.*

Proof. The proof of the theorem pretty much follows from Lemma 6.4 and Proposition 6.5. We just need to remind the reader that (6.31) can be rewritten in a polynomial form by Proposition 2.7 and we can make sure that all the variables range over $O_{K_\infty, \mathcal{W}_{K_\infty}}$ as opposed to FK_∞ or $O_{FK_\infty, \mathcal{W}_{FK_\infty}}$. This can be done using Proposition 2.6 of [33]. (For more extensive discussion of “rewriting” issues the reader can see the section on coordinate polynomials in the Appendix B of [32].) \square

To get down to \mathbb{Q} we need additional notation and assumptions.

Notation and Assumptions 6.7. We add the following to our notation and assumption list.

- Let K^{Gal} be the Galois closure of K over \mathbb{Q} .
- Assume E/\mathbb{Q} is cyclic of prime degree and $n_E > [K^{Gal} : \mathbb{Q}]$.
- Using Corollary 7.6.1 of [32] and Proposition 2.1 we know that for some set of K -primes \mathcal{T}_K such that $\mathcal{V}_K \subset \mathcal{T}_K$ and $\mathcal{T}_K \setminus \mathcal{V}_K$ is a finite set, we have that $O_{K, \mathcal{T}_K} \cap \mathbb{Q}$ has a Diophantine definition over O_{K, \mathcal{T}_K} . From Proposition 2.1 it also follows that we can add finitely many primes to \mathcal{T}_K without changing the situation. Thus for the results below it is enough to assume that \mathcal{T}_K contains all the primes of $\mathcal{T}_K \setminus \mathcal{V}_K$.
- Let $\mathcal{R}_K = \mathcal{V}_K \cup \mathcal{S}_K$.

Given the additional notation and assumptions above we now have the following corollary.

- Corollary 6.8.**
- (1) *$O_{K_\infty, \mathcal{W}_{K_\infty}} \cap \mathbb{Q}$ has a Diophantine definition over $O_{K_\infty, \mathcal{W}_{K_\infty}}$.*
 - (2) *For any archimedean and non-archimedean topology of K_∞ we can choose \mathcal{S}_K so that $O_{K_\infty, \mathcal{W}_{K_\infty}}$ has an infinite Diophantine subset which is discrete in this topology of the field.*
 - (3) *O_{K, \mathcal{W}_K} is contained in a set with a (natural or Dirichlet) density is $1 - \frac{1}{[E:\mathbb{Q}]}$.*
 - (4) *$O_{K_\infty, \mathcal{R}_{K_\infty}} \cap \mathbb{Q}$ has a Diophantine definition over $O_{K_\infty, \mathcal{R}_{K_\infty}}$ and therefore HTP is unsolvable over $O_{K_\infty, \mathcal{R}_{K_\infty}}$*
 - (5) *O_{K, \mathcal{R}_K} is contained in a set with a (natural or Dirichlet) density less or equal to $1 - \frac{1}{[K:\mathbb{Q}]} - \frac{1}{[E:\mathbb{Q}]}$.*

Proof.

- (1) This assertion follows directly from Theorem 6.6, Proposition 2.1 and Corollary 7.6.1 of [32].
- (2) This part of the corollary follows from Section 3 of [30] and Section 2 of [18].
- (3) This statement follows from the fact that the set of K primes inert in the extension EK/K has (Dirichlet or natural) density $1 - \frac{1}{[E:\mathbb{Q}]}$.
- (4) This assertion is true because by construction of \mathcal{R}_K we have that $O_{K_\infty, \mathcal{R}_{K_\infty}} \cap \mathbb{Q}$ is a “small” ring, i.e. a ring of the form $O_{\mathbb{Q}, \mathcal{T}_\mathbb{Q}}$, where $\mathcal{T}_\mathbb{Q}$ is a finite, possibly empty set of rational primes. Thus, by Proposition 2.1, \mathbb{Z} has a Diophantine definition over $\mathcal{T}_\mathbb{Q}$ and therefore over $O_{K_\infty, \mathcal{R}_{K_\infty}}$. Hence HTP is unsolvable over this ring.
- (5) This part of the corollary follows from a standard density calculation (see for example Section B.5 of [32]). \square

We restate our results in the following two formulations.

Theorem 6.9. *Let K_∞ be a totally real possibly infinite algebraic extension of \mathbb{Q} normal over some number field and such that for some rational prime number p we have that $i_{K_\infty}(p) = 0$. Let U_∞ be a finite extension of K_∞ such that there exists an elliptic curve \mathbf{E} defined over U_∞ with $\mathbf{E}(U_\infty)$ finitely generated and of a positive rank. Then K_∞ contains a large subring R such that \mathbb{Z} is definable over R and HTP is unsolvable over R .*

Theorem 6.10. *Let K_∞ be a totally real possibly infinite algebraic extension of \mathbb{Q} normal over some number field and such that there exists a non-repeating sequence of rational prime numbers $\{p_i\}$ with the property that $i_{K_\infty}(p_i) < \infty$. Let U_∞ be a finite extension of K_∞ such that there exists an elliptic curve \mathbf{E} defined over U_∞ with $\mathbf{E}(U_\infty)$ finitely generated. Then for any $\varepsilon > 0$ we have that K_∞ contains a large subring R satisfying the following conditions:*

- (1) *There exists a number field $K \subset K_\infty$ and a set $\mathcal{W}_K \subset \mathcal{P}(K)$ of (Dirichlet or natural) density greater than $1 - \varepsilon$ such that $R = O_{K_\infty, \mathcal{W}_{K_\infty}}$.*
- (2) *\mathbb{Z} is definable over R and HTP is unsolvable over R .*

Before stating the theorem concerning arbitrary small rings we change assumptions again.

Notation and Assumptions 6.11. We will now remove conditions imposed on \mathcal{S}_K in Notation and Assumptions 6.7. That is in what follows we again assume that \mathcal{S}_K is an arbitrary finite set of primes of K .

First as a consequence of Theorem 6.6 we have the following corollary.

Corollary 6.12. *\mathbb{Z} , $O_{K_\infty, \mathcal{S}_{K_\infty}} \cap \mathbb{Q}$ and O_{K, \mathcal{S}_K} have Diophantine definitions over $O_{K_\infty, \mathcal{S}_{K_\infty}}$. Thus HTP is not solvable over $O_{K_\infty, \mathcal{S}_{K_\infty}}$.*

This result can also be restated in the following form.

Theorem 6.13. *Let K_∞ be a totally real possibly infinite algebraic extension of \mathbb{Q} normal over some number field and such that for some rational prime number p we have that $i_{K_\infty}(p) = 0$. Let U_∞ be a finite extension of K_∞ such that there exists an elliptic curve \mathbf{E} defined over U_∞ with $\mathbf{E}(U_\infty)$ finitely generated. Then for any small subring R of K_∞ we have that \mathbb{Z} is definable over R and HTP is unsolvable over R .*

7. DIOPHANTINE DEFINITION OF RATIONAL INTEGERS FOR EXTENSIONS OF DEGREE 2 OF TOTALLY REAL FIELDS.

Most of the work necessary for treating the case of extensions of degree 2 of the totally real fields discussed above has been done in [33]. However we will revisit some of the results because in the current case the presentation can be simplified and the results concerning rings of integers can be made slightly more general. We start, as usual with notation and assumptions.

Notation and Assumptions 7.1. In this section we make the following changes and additions to the notation and assumption list.

- For the case of integers we remove all the assumptions on K_∞ besides the fact that it is an algebraic possibly infinite extension of \mathbb{Q} and K contains a totally positive element (that is an element all of whose \mathbb{Q} -conjugates are positive) which is not a square in K_∞ .
- Let G be an extension of degree 2 of K . Let α_G be a generator of G over K with $\alpha_G^2 = a_G \in O_K$. Assume G is not a totally real field.
- Assume $[GK_\infty : K_\infty] = 2$.
- Let $d_H \in O_K$ be such that it is not a square in K_∞ and all the conjugates of d_H over \mathbb{Q} are greater than 1 in absolute value.
- Assume that for any embedding $\sigma : K \rightarrow \mathbb{C}$ we have that $\sigma(d_H) > 0$ if and only if $\sigma(a_G) < 0$.
- Let $\delta_H \in \mathbb{C}$ be a square root of d_H .
- Let $H = K(\delta_H)$.
- Given a number field T we let U_T denote the group of integral units of T , let s_T denote the number of non-real embeddings of T into \mathbb{C} , and let r_T denote the number of real embeddings of T into \mathbb{C} .
- Let M as before be a number field contained in K_∞ and containing K .

Remark 7.2. d_H as described above exists by the Strong Approximation Theorem and our assumptions.

We start our discussions of technical details with a proposition due to Denef and Lipshitz in [6].

Proposition 7.3. *Let $M \subset K_\infty$ be a number field with $K \subseteq M$. Let*

$$A_{GM} = \{\varepsilon \in U_{GHM} : \mathbf{N}_{GHM/GM}(\varepsilon) = 1\}$$

$$A_M = \{\varepsilon \in U_{HM} : \mathbf{N}_{HM/M}(\varepsilon) = 1\}$$

Then A_{GM} and A_M are multiplicative groups of equal rank.

From this proposition we derive the following corollary.

Corollary 7.4. *Let*

$$B_{GM} = \{x + \delta_H y : x, y \in O_G, x + \delta_H y \in A_{GM}\},$$

$$B_M = \{x + \delta_H y : x, y \in O_M, x + \delta_H y \in A_M\}.$$

Then if $x + \delta_H y \in B_{GM}$, it follows that $(x + \delta_H y)^4 \in B_M$. Further, assuming that $[M : \mathbb{Q}] \geq 2$ we have that B_M contains elements of infinite order.

Proof. Let σ_G be the generator of $\text{Gal}(GM/M)$ and let σ_H be a generator of $\text{Gal}(HM/M)$. We can extend both elements to GHM by requiring σ_G to be the identity on H and similarly σ_H to be the identity on G . Then we observe that $\text{Gal}(GHM/M)$ is generated by σ_G and σ_H and $\sigma_G \sigma_H = \sigma_H \sigma_G$.

Now let $\varepsilon \in A_{GM}$. Then $\sigma_G(\varepsilon) \in A_{GM}$. Indeed, $\varepsilon \in A_{GM}$ if and only if $\varepsilon \sigma_H(\varepsilon) = 1$. Therefore we have the following equality:

$$\sigma_G(\varepsilon) \sigma_H(\sigma_G(\varepsilon)) = \sigma_G(\varepsilon \sigma_H(\varepsilon)) = 1.$$

Given our definition of $B_{GM} = A_{GM} \cap O_G[\delta_H]$, it also follows that $\varepsilon \in B_{GM}$ if and only if $\sigma_G(\varepsilon) \in B_{GM}$. Further, it is also the case that $\varepsilon \in B_{GM}$ if and only if $\varepsilon^{-1} \in B_{GM}$. Finally it is clear that B_{GM} is a multiplicative group and from Proposition 7.3 we have that for any $\varepsilon \in B_{GM}$ for some l it is the case that $\varepsilon^l \in B_M$ and consequently $\varepsilon^l = \sigma_G(\varepsilon)^l$. Thus, $\frac{\varepsilon}{\sigma_G(\varepsilon)} = \xi_l$, where ξ_l is a root of unity which is also an element of B_{GM} . By Lemma 11.3, $\xi_l^4 = 1$. Thus our first assertion is true.

Next we observe that given our assumption on $[M : \mathbb{Q}]$ we have that A_M has elements of infinite order. Finally, by Lemma 6.1.4 and Lemma B.4.12 of [32], we conclude that B_M has elements of infinite order. \square

Next for the convenience of the reader we state two technical lemmas which are simplified versions of results in [33] concerning bounds.

Lemma 7.5. *Let $x = y_0 + y_1 \alpha_G \equiv z \pmod{\mathfrak{Z}}$ in O_{GHM} where $x \in O_{GM}, y_0, y_1 \in O_M, z \in O_{HM}, \mathfrak{Z}$ an integral divisor of HM . Let $Z = \mathbf{N}_{GHM/\mathbb{Q}}(\mathfrak{Z})$. Then $\frac{\mathbf{N}_{GHM/\mathbb{Q}}(2\alpha y_1)}{Z}$ is an integer.*

(See Lemma 6.6 of [33].)

Lemma 7.6. *Let $x \in GM, x = y_0 + \alpha_G y_1, y_1, y_2 \in M, z \in GM$. Suppose further that for any σ , an embedding of GM into \mathbb{R} , we have that*

$$1 \leq |\sigma(x)| < |\sigma(z)|$$

while for any τ , a non-real embeddings of GM into \mathbb{C} , we have that

$$\tau(z) \geq 1.$$

Then $|\mathbf{N}_{GM/\mathbb{Q}}(y_1)| \leq |\mathbf{N}_{GM/\mathbb{Q}}(x)| |\mathbf{N}_{GM/\mathbb{Q}}(z)|$.

(See Lemma 6.9 of [33].)

Lemma 7.7. *Let $\varepsilon \in B_K$. Then for any positive integer k and any $\lambda > 0$ there exists a positive integer r such that for all $\tau : H \rightarrow \mathbb{C}$ with $\tau(H) \not\subseteq \mathbb{R}$ we have that*

$$\left| \frac{\tau(\varepsilon^{rk} - 1)}{\tau(\varepsilon^r - 1)} - k \right| < \lambda.$$

(See Lemma 7.2 of [33].)

We are now ready to list the equations comprising a Diophantine definition we seek.

Theorem 7.8. *There exists a polynomial equation $P(x, \bar{t}) \in O_K[x, \bar{t}]$ such that the following statements are true.*

- (1) *For any $x \in O_{GK_\infty}$, if $P(x, \bar{t}) = 0$ for some $\bar{t} = (t_1, \dots, t_m)$ with $t_i \in O_{GK_\infty}$, then $x \in O_{K_\infty}$.*
- (2) *If $x \in \mathbb{Z}$ there exists $\bar{t} = (t_1, \dots, t_m)$ with $t_i \in O_K$ such that $P(x, \bar{t}) = 0$*

Proof. The proof will use Proposition 7.3 of [33] as its foundation. However, our notation is a bit different from the notation used in that proposition. Let $x \in O_{GK_\infty}$, $a_1, a_2, b_1, b_2, c_1, d_1, \dots, c_4, d_4, u, v, u_1, v_1, \dots, u_4, v_4 \in O_{GK_\infty}$, $\gamma_1, \dots, \gamma_4 \in O_{GHK_\infty}$, and assume the following conditions and equations are satisfied.

$$(7.1) \quad u_i^2 - d_H v_i^2 = 1, i = 1, \dots, 4,$$

$$(7.2) \quad \gamma_i = (u_i - \delta_H v_i)^4, i = 1, \dots, 4,$$

$$(7.3) \quad \frac{\gamma_{2j} - 1}{\gamma_{2j-1} - 1} = a_j - \delta_H b_j, j = 1, 2$$

$$(7.4) \quad \gamma_i = c_i + \delta_H d_i, i = 1, \dots, 4,$$

$$(7.5) \quad 1 \leq |\sigma(x)| \leq 1 + \sigma(a_1^2 - d_H b_1^2)^2,$$

where σ ranges over all embeddings of GK_∞ into \mathbb{R} ,

$$(7.6) \quad x - (a_2 - \delta_H b_2) = (c_3 - 1 + \delta_H d_3)(u + v\delta_H),$$

$$(7.7) \quad 6\alpha_G x(1 + (a_1^2 - d_H b_1^2)^2) | (c_3 - 1 + \delta_H d_3).$$

Then, we claim, $x \in O_{K_\infty}$.

Conversely, we claim that if $x \in \mathbb{Z}_{>0}$, the conditions and equations above can be satisfied with $a_1, a_2, b_1, b_2, c_1, d_1, \dots, c_4, d_4, u, v, u_1, v_1, z_1, \dots, u_4, v_4, \gamma_i \in O_{HK}, i = 1, \dots, 4$.

To prove the first claim, observe the following. Let M be such that HGM contains $\alpha_G, \delta_H, x, a_1, a_2, b_1, b_2, c_1, d_1, \dots, c_4, d_4, u, v, u_1, v_1, \dots, u_4, v_4, \gamma_1, \dots, \gamma_4$. Then given our assumptions on the fields under consideration, in the equations above we can replace HGK_∞ by HGM , GK_∞ by GM , and finally K_∞ by M , while the equalities and other conditions will continue to be true.

By Corollary 7.4 and equations (7.1) and (7.2) we have that $\gamma_1, \dots, \gamma_4 \in HM$, and consequently from equation (7.3) we also have that $a_j^2 - d_H b_j^2 \in M$ for $j = 1, 2$. From equation (7.5) we know that

$$1 \leq \sigma(x) \leq 1 + \sigma(a_1^2 - d_H b_1^2)^2$$

for all real embeddings σ of GM . Next observe that

$$x - (a_2 - \delta_H b_2) \equiv 0 \pmod{(\gamma_3 - 1)},$$

and therefore if $x = y_0 + y_1 \alpha_G, y_0, y_1 \in M$, by Lemma 7.5 we have that

$$\mathbf{N}_{HGM/\mathbb{Q}}(2y_1 \alpha_G) \equiv 0 \pmod{\mathbf{N}_{HGM/\mathbb{Q}}(\gamma_3 - 1)}.$$

So either $y_1 = 0$ or

$$\mathbf{N}_{HGM/\mathbb{Q}}(2y_1 \alpha_G) \geq \mathbf{N}_{HGM/\mathbb{Q}}(\gamma_3 - 1).$$

Observe that for any $\tau : GM \rightarrow \mathbb{C} \setminus \mathbb{R}$ we have that $|\tau(1 + (a_1^2 - d_H b_1^2)^2)| \geq 1$ since $\tau(a_1^2 - d_H b_1^2) \in \mathbb{R}$. Thus by Lemma 7.6, equation (7.5) and equation (7.7) we have that

$$\mathbf{N}_{HGM/\mathbb{Q}}(2\alpha_G y_1) \leq \mathbf{N}_{HGM/\mathbb{Q}}(2\alpha_G) \mathbf{N}_{HGM/\mathbb{Q}}(x) \mathbf{N}_{GMH/\mathbb{Q}}(1 + (a_1^2 - d_H b_1^2)^2) < \mathbf{N}_{GMH/\mathbb{Q}}(\gamma_3 - 1).$$

Therefore unless $y_1 = 0$, we have a contradiction.

We will now show that assuming that $x > 1$ is a natural number, we can satisfy all the equations and conditions (7.1)–(7.7). Let $\nu \in B_K$ be a unit of O_H which is not a root of unity. Such a ν exists by Corollary 7.4. Let $\{\phi_1, \dots, \phi_{s_H}\}$ be a set containing a representative from every complex-conjugate pair of non-real

conjugates of ν . By Lemma 7.7, we can find a positive integer $r \cong 0 \pmod{4}$ such that for all $i = 1, \dots, s_H$ we have that

$$\left| \frac{\phi_i^{rx} - 1}{\phi_i^r - 1} - x \right| < \frac{1}{2},$$

and thus,

$$\left| \frac{\phi_i^{rx} - 1}{\phi_i^r - 1} \right| > x - \frac{1}{2}.$$

So we set $u_1 - \delta_H v_1 = \nu^{r/4}$, $\gamma_1 = \nu^r$, $u_2 - \delta_H v_2 = \nu^{rx/4}$, $\gamma_2 = \nu^{rx}$. Then for $i = 1, 2$ equation (7.1) is satisfied. We also satisfy (7.2) for these values of i . Next we define a_1 and b_1 so that (7.3) is satisfied for $j = 1$. Next let σ be an embedding of M into \mathbb{R} extending to a real embedding of GM and therefore corresponding to a real embedding of G . Then by assumption on H , we have that σ extends to a non-real embedding $\hat{\sigma}$ on HM . Thus, without loss of generality, for some $i = 1, \dots, s_H$ we have that

$$\hat{\sigma}(a_1 - \delta_H b_1) = \hat{\sigma} \left(\frac{\nu^{rx} - 1}{\nu^r - 1} \right) = \frac{\phi_i^{rx} - 1}{\phi_i^r - 1},$$

and therefore

$$\sigma(a_1^2 - d_H b_1^2) = \left| \frac{\phi_i^{rx} - 1}{\phi_i^r - 1} \right|^2 > x - \frac{1}{2},$$

leading to

$$1 + \sigma(a_1^2 - d_H b_1^2)^2 > x = \sigma(x) > 1.$$

Thus we can satisfy (7.5).

Let $\nu_3 \in B_K$, assume ν_3 is not a root of unity, and let $\nu_3 = u_3 - \delta_H v_3$ with $u_3, v_3 \in O_M[\delta_H]$ be such that

$$(7.8) \quad \nu_3 - 1 \equiv 0 \pmod{6a_G x(1 + (a_1^2 - d_H b_1^2)^2)}$$

This can be done by Corollary 7.4 and by Section 2.1.1 of [28]. Set $\gamma_3 = \nu_3^4$. Then (7.1), (7.2), and (7.4) for $i = 3$ are satisfied. Finally, set $\gamma_4 = \gamma_3^x$, $\nu_4 = \nu_3^x$. In this case we can satisfy (7.1), (7.2), and (7.4) for $i = 4$. We now observe that

$$a_2 - \delta b_2 = \frac{\gamma_4 - 1}{\gamma_3 - 1} = x + (\gamma_3 - 1)(u + \delta_H v) = x + (c_3 - 1 - \delta_H d_3)(u + v\delta_H),$$

where $u, v \in O_K$. Thus (7.6) will also be satisfied. The only remaining issue is to note that from the discussion of Section 2 we can rewrite all the equations and conditions as polynomial equations with variables taking values in O_{GK_∞} . This can be done using Propositions 2.6 – 2.8 of [33]. \square

We can now state the main theorem of this section.

Theorem 7.9. *Let K_∞ be a totally real possibly infinite algebraic extension of \mathbb{Q} . Let U_∞ be a finite extension of K_∞ such that there exists an elliptic curve \mathbf{E} defined over U_∞ with $\mathbf{E}(U_\infty)$ finitely generated and of a positive rank. Let GK_∞ be an extension of degree 2 over K_∞ . If GK_∞ has no real embeddings, assume additionally that K_∞ has a totally real extension of degree 2. Then \mathbb{Z} is existentially definable and HTP is unsolvable over the ring of integers of GK_∞ .*

8. DIOPHANTINE DEFINITION OF SOME LARGE RATIONAL SUBRINGS AND ARBITRARY SMALL SUBRINGS FOR EXTENSIONS OF DEGREE 2 OF TOTALLY REAL FIELDS.

In this section we will prove a result analogous to Theorem 7.9 for some big and arbitrary small subrings of K_∞ under some assumptions on the field under consideration. As in the case of the ring of integers most of the work has already been done for this case in [33] but we will have to adjust notation and some details.

Notation and Assumptions 8.1. We now bring back all the assumptions we had concerning K_∞ as in Notation and Assumptions 6.1 and 6.7. We also continue to use notation and assumptions from 7.1 except for the first item which deals with K_∞ . Finally we add the following to our notation and assumptions list.

- Let \mathcal{Z}_K be a subset of \mathcal{V}_K such that the primes of \mathcal{Z}_K do not split in the extension G/K and do not divide the discriminant of $R(X)$.
- For any number field M with $K \subset M \subset K_\infty$, assume that $[M : K]$ is odd. (By Lemma 11.2 this assumption implies that primes of \mathcal{Z}_M remain inert in the extension GM/M .)

- Assume that at least two K -primes \mathfrak{q}_1 and \mathfrak{q}_2 lying above two different rational primes are not ramified in K_∞ .
- Assume that the field $EHGK_\infty$ contains no roots of unity which are not already in EGK_∞ . (The lemma below assures us that we can arrange this under our assumptions.)
- Let p be any rational prime without any factors in \mathcal{Z}_K and such that $p > |\phi(\alpha_G)|$ for any ϕ , an embeddings of K into its algebraic closure.

Proposition 8.2. *There exists a number field H satisfying all the requirements from Notation and Assumptions 7.1 and 8.1.*

Proof. Let $a_1, a_2 \in O_K$ be such that $\text{ord}_{\mathfrak{q}_i} a_i = 1$. By the Strong approximation theorem we can find $d_H \in O_K$ in such that its conjugates over \mathbb{Q} have the right sign and such that $\text{ord}_{\mathfrak{q}_i}(d_H - a_i) > 2$ for $i = 1, 2$. The last requirement will make sure that $\text{ord}_{\mathfrak{q}_i} d_H = 1$ and factors of two primes are ramified in the extension $EHGK_\infty/EGK_\infty = EGK_\infty(\delta_H)/HGK_\infty$. This is enough to make sure that this extension of degree 2 is not generated by any root of unity. (See Lemma 2.4 of [25].) \square

To prove our results we will need the following technical propositions from [33].

Proposition 8.3. *Consider the following system of equations where M , as usual, is a number field with $K \subseteq M \subset K_\infty$.*

$$(8.1) \quad \begin{cases} \mathbf{N}_{EHGM/EGM}(\varepsilon) = 1 \\ \mathbf{N}_{EHGM/HGM}(\varepsilon) = 1 \end{cases}$$

We claim that any for $\varepsilon \in O_{EHGM, \mathcal{Z}_{EHGM}}$ satisfying (8.1) we have that $\varepsilon^2 \in O_{HME}$. Further, there is always $\varepsilon \in U_{HME}$ such that it is not a root of unity and is a solution to the system.

(See Lemma 5.3 and Corollary 5.4 of [33] for a proof.)

Lemma 8.4. *Let $x \in O_{GM, \mathcal{Z}_{GM}}$, $x = y_0 + y_1 \alpha_G \equiv z \pmod{\mathfrak{Z}}$ in $O_{HEGM, \mathcal{Z}_{HEGM}}$, where $z \in O_{HEM, \mathcal{Z}_{HEM}}$, $y_0, y_1 \in M$, \mathfrak{Z} is an integral divisor of HEM without any factors in $\overline{\mathcal{Z}}_{HEM}$. Assume additionally that for any $\mathfrak{t} \in \overline{\mathcal{Z}}_{GEM}$ we have that $\text{ord}_{\mathfrak{t}} x \leq 0$. Let $\mathbf{N}_{HEGM/\mathbb{Q}}(x) = \frac{X}{Y}$, where $X, Y \in \mathbb{Z}$ and $(X, Y) = 1$ in \mathbb{Z} . Let $Z = \mathbf{N}_{HEGM/\mathbb{Q}}(\mathfrak{Z})$. Then $\frac{Y}{Z} \mathbf{N}_{HEGM/\mathbb{Q}}(2\alpha y_1)$ is an integer.*

(See Lemma 6.6 of [33] for proof.)

We are now ready to state the main result of this section whose proof is similar to the proof of Proposition 10.5 in [33]. However, as usual, some details need to be changed.

Theorem 8.5. *There exists a polynomial equation $P(x, \bar{t}) \in O_K[x, \bar{t}]$ such that the following statements are true.*

- (1) *For any $x \in O_{GK_\infty, \mathcal{Z}_{GK_\infty}}$, if $P(x, \bar{t}) = 0$ for some $\bar{t} = (t_1, \dots, t_m)$ with $t_i \in O_{GK_\infty, \mathcal{Z}_{GK_\infty}}$, then $x \in O_{K_\infty, \mathcal{Z}_{K_\infty}}$.*
- (2) *If $x \in \mathbb{Z}$ then there exists $\bar{t} = (t_1, \dots, t_m)$ with $t_i \in O_{K, \mathcal{Z}_K}$ such that $P(x, \bar{t}) = 0$*

Proof. Let $x_0, x_1 \in O_{G_\infty, \mathcal{Z}_{G_\infty}}$, $a_1, a_2, b_1, b_2, c_1, d_1, \dots, c_4, d_4, u, v \in O_{EG_\infty, \mathcal{Z}_{EG_\infty}}$, $\varepsilon_i, \gamma_i \in O_{EHGK_\infty, \mathcal{Z}_{EHGK_\infty}}$, $i = 1, \dots, 4$, and assume the following conditions and equations are satisfied.

$$(8.2) \quad x_1 = R(x_0),$$

$$(8.3) \quad \begin{cases} \mathbf{N}_{HEGK_\infty/EGK_\infty}(\varepsilon_i) = 1, i = 1, \dots, 4, \\ \mathbf{N}_{HEGK_\infty/HGK_\infty}(\varepsilon_i) = 1, i = 1, \dots, 4, \end{cases}$$

$$(8.4) \quad \gamma_i = \varepsilon_i^2, i = 1, \dots, 4,$$

$$(8.5) \quad \frac{\gamma_{2j} - 1}{\gamma_{2j-1} - 1} = a_j - \delta_H b_j, j = 1, 2$$

$$(8.6) \quad \gamma_i = c_i + \delta_H d_i, i = 1, \dots, 4,$$

$$(8.7) \quad 1 \leq |\sigma(x_1)| \leq R(A(1) + \sigma(a_1^2 - d_H b_1^2)^2),$$

where σ ranges over all embeddings of EGK_∞ into \mathbb{R} ,

$$(8.8) \quad x_1 - (a_2 - \delta_H b_2) = (c_3 - 1 + \delta_H d_3)(u + v\delta_H),$$

$$(8.9) \quad p^2 x_1 R(A(1) + (a_1^2 - d_H b_1^2)^2) | (c_3 - 1 + \delta_H d_3).$$

Then, we claim, $x_1 \in K_\infty$.

Conversely, we claim that if $x_0 \in \mathbb{Z}_{>1}$, the conditions and equations above can be satisfied with $a_1, a_2, b_1, b_2, c_1, d_1, \dots, c_4, \dots, d_4, u, v \in O_{EK, \mathcal{Z}_{EK}}, \gamma_i, \varepsilon_i \in O_{EMHK, \mathcal{Z}_{EH}}, i = 1, \dots, 4$.

To prove the first claim, observe the following. Let M be such that $GHEM$ contains $\alpha_G, \delta_H, \mu_E, x_0, a_1, a_2, b_1, b_2, c_1, d_1, \dots, c_4, d_4, u, v, \varepsilon_1, \dots, \varepsilon_4$. Then given our assumptions on the fields under consideration, in the equations above we can replace $EHGK_\infty$ by $EHGM$, EGK_∞ by EGM , and finally K_∞ by M , while the equalities and other conditions will continue to be true, assuming we modify the prime sets by choosing the primes in the finite extensions so that $O_{GK_\infty, \mathcal{Z}_{GK_\infty}}$ is the integral closure of $O_{GM, \mathcal{Z}_{GM}}$, $O_{EGK_\infty, \mathcal{Z}_{EGK_\infty}}$ is the integral closure of $O_{EGM, \mathcal{Z}_{EGM}}$, and $O_{EHGK_\infty, \mathcal{Z}_{EHGK_\infty}}$ is the integral closure of $O_{EGHM, \mathcal{Z}_{EGHM}}$ in GK_∞, EGK_∞ and $EHGK_\infty$ respectively. Then by Proposition 8.3 we know that $\gamma_i \in HEM \subset HEK_\infty$. Since δ_H generates HEM over EM as well as $HEGM$ over EGM , we conclude that $c_i, d_i \in O_{EM, \mathcal{Z}_{EM}}$ for $i = 1, \dots, 4$. A similar argument tells us that $a_1, b_1, a_2, b_2 \in O_{EM, \mathcal{Z}_{EM}}$.

Next from (8.2) and Lemma 2.9 we conclude that for all $\mathfrak{p} \in \mathcal{Z}_{EGM}$ we have that $\text{ord}_{\mathfrak{p}} x_1 \leq 0$ and

$$\text{ord}_{\mathfrak{p}} R(A(1) + (a_1^2 - d_H b_1^2)^2) \leq 0.$$

From the definition of $A(1)$ and the fact that $a_1, b_1 \in EM$ - a totally real field, we have that

$$(8.10) \quad 1 \leq R(A(1) + \tau(a_1^2 - d_H b_1^2)^2),$$

where τ ranges over all non-real embeddings of EGM into \mathbb{C} . Combining the bound equations (8.7) and (8.10), and writing $x_1 = y_0 + y_1 \alpha_G$, where $y_0, y_1 \in O_{M, \mathcal{Z}_M}$, we conclude by Lemma 7.6

$$(8.11) \quad |\mathbf{N}_{EGM/\mathbb{Q}}(y_1)| \leq |\mathbf{N}_{EGM/\mathbb{Q}}(x_1) \mathbf{N}_{EGM/\mathbb{Q}}(R(A(1) + (a_1^2 - d_H b_1^2)^2))|.$$

Let $\mathfrak{D} = \mathfrak{n}_{EGHM, \overline{\mathcal{Z}_{EGHM}}}(c_3 - 1 + \delta_H d_3)$. Note that since $c_3 - 1 + \delta_H d_3 \in HEM$ and $\overline{\mathcal{Z}_{HEGM}}$ is closed under conjugation over \mathbb{Q} and thus over HEM , we can regard \mathfrak{D} as a divisor of HEM . Observe further that from (8.8), we have that \mathfrak{D} divides $\mathfrak{n}_{GHEM}(x_1 - (a_2 - b_2 \delta_H))$. Let

$$D = |\mathbf{N}_{HEGM/\mathbb{Q}}(\mathfrak{D})| \in \mathbb{Z}_{>0},$$

let

$$|\mathbf{N}_{HEGM/\mathbb{Q}}(x_1)| = \frac{X}{Y},$$

and let

$$|\mathbf{N}_{HEGM/\mathbb{Q}}(A(1) + R(a_1^2 - d_H b_1^2)^2)| = \frac{U}{V},$$

where $X, Y, U, V \in \mathbb{Z}_{>0}$, $(X, Y) = 1$, $(U, V) = 1$, and X, U are not divisible by any rational primes with factors in \mathcal{Z}_{HEGM} . Then from (8.9) we have that

$$(8.12) \quad \mathbf{N}_{EGHM/\mathbb{Q}}(2\alpha_G) X U < \mathbf{N}_{EGHM/\mathbb{Q}}(p^2) X U < D.$$

Note that by Lemma 11.2 we have that all the primes of \mathcal{Z}_M do not split in the extension GM/M and therefore by Lemma 8.4, on the one hand we have that

$$\frac{Y \mathbf{N}_{GHME/\mathbb{Q}}(2\alpha_G y_1)}{D} \in \mathbb{Z},$$

and therefore

$$|Y \mathbf{N}_{GHME/\mathbb{Q}}(2\alpha_G y_1)| \geq D \text{ or } y_1 = 0.$$

On the other hand, combining (8.11) and (8.12), we have that

$$|Y \mathbf{N}_{GHME/\mathbb{Q}}(2\alpha_G y_1)| \leq |\mathbf{N}_{EGHM/\mathbb{Q}}(2\alpha_G) X U| < D.$$

Thus y_1 is 0 and $x_1 \in M$.

We will now show that assuming that $x_0 > 1$ is a natural number, we can satisfy all the equations and conditions (8.2)–(8.9) with all the variables ranging over the appropriate sets. Observe that by (8.2), we have that x_1 is also a natural number. Let $\nu \in U_{HE} \cap O_K[\delta_H, \mu_E]$ be a solution to (8.3) such that it is not a root of unity. Such a solution exists by Proposition 8.3 and by Section 2.1.1 of [28]. Let $\{\phi_1, \dots, \phi_{s_{HE}}\}$ be a set containing a representative from every complex-conjugate pair of non-real conjugates of ν . By Lemma 7.7, we can find a positive integer $r \equiv 0 \pmod{2}$ such that for all $i = 1, \dots, s_{HE}$ we have that

$$\left| \frac{\phi_i^{rA} - 1}{\phi_i^r - 1} - A \right| < \frac{1}{2},$$

where $A = A(x_1) + 1$, and thus,

$$\left| \frac{\phi_i^{rA} - 1}{\phi_i^r - 1} \right| > A - \frac{1}{2} > A(x_1).$$

So we set $\varepsilon_1 = \nu^{r/2}$, $\gamma_1 = \varepsilon^r$, $\varepsilon_2 = \varepsilon^{rA/2}$, $\gamma_2 = \varepsilon^{rA}$. Then for $i = 1, 2$ the system (8.3) is satisfied. We also satisfy (8.4) for these values of i . Next we define a_1 and b_1 so that (8.5) is satisfied for $j = 1$. Next let σ be an embedding of K into \mathbb{R} extending to a real embedding of G and therefore to a real embedding of GE . Then by assumption on H , we have that σ extends to a non-real embedding $\hat{\sigma}$ on HE . Thus, without loss of generality, for some $i = 1, \dots, s_{HE}$ we have that

$$\hat{\sigma}(a_1 - \delta_H b_1) = \hat{\sigma} \left(\frac{\varepsilon^{rA} - 1}{\varepsilon^r - 1} \right) = \frac{\phi_i^{rA} - 1}{\phi_i^r - 1},$$

and therefore

$$\sigma(a_1^2 - d_H b_1^2) = \left| \frac{\phi_i^{rA} - 1}{\phi_i^r - 1} \right|^2 > A(x_1)^2 > A(x_1),$$

leading to

$$Q(A(1) + \sigma(a_1^2 - d_H b_1^2)) > x_1 = \sigma(x_1) > 1.$$

Thus we can satisfy (8.7).

Now let ε_3 to be a solution to (8.3) in $O_K[\delta_H, \mu_E]$ such that $\gamma_3 = \varepsilon_3^2 \in U_{HE} \cap O_K[\delta_H, \mu_E]$, (8.4), (8.6) for $i = 3$, and (8.9) are satisfied. Again this can be done by Proposition 8.3 and by Section 2.1.1 of [28]. Finally, set $\varepsilon_4 = \varepsilon_3^{x_1}$, $\gamma_4 = \gamma_3^{x_1}$. In this case we can satisfy (8.3), (8.4) for $i = 4$.

We now observe that

$$a_2 - \delta_H b_2 = \frac{\gamma_4 - 1}{\gamma_3 - 1} = x_1 + (\gamma_3 - 1)(u + \delta_H v) = x_1 + (c - 1 - \delta_H d)(u + v\delta_H),$$

where $u, v \in O_{GM, \mathcal{U}_{GM}}[\mu_E]$. Thus (8.8) will also be satisfied. As a last step we select $c_1, d_1, \dots, c_4, d_4 \in O_M$ so that (8.6) is satisfied. The only remaining issue is to note that we can rewrite all the equations and conditions as polynomial equations with variables taking values in GK_∞ (see Propositions 2.6 – 2.8 of [33] again), and also to observe that we can require $x_0 + 1, \dots, x_0 + n_E$ to satisfy the equations above. Making sure that $x_0, x_0 + 1, \dots, x_0 + n_E \in K_\infty$ is enough by Lemma 5.1 of [26] to insure that x_0 is in K_∞ . \square

Our next task is to go down to \mathbb{Q} . Unfortunately as in Section 6 there are technical complications which will force us to modify the prime sets allowed in the denominators of the divisors of ring elements. The problem lies in the fact that we might have to add a finite set of primes to \mathcal{Z}_K in order to go down to \mathbb{Q} . In the case of the totally real fields we just needed to make sure that in Proposition 6.5 the “key” variable x_j did not have the “extra” primes in the denominator of its divisor. This was accomplished by using the fact that any finite set of primes over the field under consideration was boundable. Unfortunately, in this case we have another problem to worry about: extra solutions to the norm equations. This is the same problem which we encountered in [33]. To avoid the extra solutions we will have to introduce another extension $\bar{E}K$ of K which will be totally real and linearly disjoint from $GHEK_\infty$ over K .

Notation and Assumptions 8.6. Below we list our additional notation and assumptions.

- Let \bar{E} be a totally real number field of prime degree $n_{\bar{E}} > [K^{\text{Gal}} : \mathbb{Q}]$ with $(n_{\bar{E}}, n_E) = 1$.
- Let \mathcal{N}_K be a set of K -primes remaining inert in the extension $\bar{E}K/K$.

- Let \mathcal{T}_K be a set of K primes such that $O_{K, \mathcal{N}_K \cup \mathcal{T}_K} \cap \mathbb{Q}$ has a Diophantine definition over $O_{K, \mathcal{N}_K \cup \mathcal{T}_K}$. (Such a set \mathcal{T}_K exists by Corollary 7.6.1 of [32].)
- Let \mathcal{S}_K be a finite set of K primes and note that by Proposition 2.1 we also have that $O_{K, \mathcal{N}_K \cup \mathcal{T}_K \cup \mathcal{S}_K} \cap \mathbb{Q}$ has a Diophantine definition over $O_{K, \mathcal{N}_K \cup \mathcal{T}_K \cup \mathcal{S}_K}$.
- Assume that $\mathcal{T}_K \cup \mathcal{N}_K \cup \mathcal{S}_K = \mathcal{Z}_K$.

Given our assumptions we immediately have the following corollary.

Corollary 8.7. $O_{GK_\infty, \mathcal{Z}_{GK_\infty}} \cap \mathbb{Q}$ has a Diophantine definition over $O_{GK_\infty, \mathcal{Z}_{GK_\infty}}$.

From this corollary standard techniques produce the following consequences.

Corollary 8.8. (1) For any archimedean or non-archimedean topology of GK_∞ we can select \mathcal{S}_K so that $O_{GK_\infty, \mathcal{Z}_{GK_\infty}}$ has an infinite Diophantine subset discrete in this topology.

(2) \mathbb{Z} is definable over $O_{GK_\infty, \mathcal{Z}_{GK_\infty} \cup \mathcal{T}_K \cup \mathcal{S}_K}$ and HTP is not decidable over $O_{GK_\infty, \mathcal{Z}_{GK_\infty} \cup \mathcal{T}_K \cup \mathcal{S}_K}$.

(See, [18], [33] or [32].)

Finally we restate our results in the following form.

Theorem 8.9. Let K_∞ be a totally real possibly infinite algebraic extension of \mathbb{Q} , normal over some number field K , with an odd rational prime p of 0 degree index relative to K_∞ such that $p > [K^{\text{Gal}} : \mathbb{Q}]$, and with a 0 degree index for 2. Let U_∞ be a finite extension of K_∞ such that there exists an elliptic curve \mathbf{E} defined over U_∞ with $\mathbf{E}(U_\infty)$ finitely generated and of a positive rank. Let GK_∞ be an extension of degree 2 over K_∞ .

- (1) GK_∞ contains a big ring where \mathbb{Z} is existentially definable and HTP is unsolvable.
- (2) \mathbb{Z} is definable and HTP is unsolvable over any small subring of GK_∞ .

Proof. (1) Let $K \subset K_\infty$ and p be as in the statement of the theorem. Next pick a totally real cyclic extension \bar{E} of \mathbb{Q} so that $[\bar{E} : \mathbb{Q}]$ is a prime number greater than $[K^{\text{Gal}} : \mathbb{Q}]$ and is different from p . Let \mathcal{M}_K be a set of primes inert in the extension $\bar{E}K/K$. Let \mathcal{T}_K be defined as in Notation and Assumptions 8.6 so that $O_{K, \mathcal{M}_K \cup \mathcal{T}_K} \cap \mathbb{Q}$ has a Diophantine definition over $O_{K, \mathcal{M}_K \cup \mathcal{T}_K}$, and let \mathcal{S}_K be an arbitrary set of primes. Then by Lemma A9 of [33] there exists a totally real cyclic extension E of \mathbb{Q} of degree p such that no prime of $\mathcal{T}_K \cup \mathcal{S}_K$ splits in the extension EK/K . Further E and \bar{E} will satisfy Notation and Assumptions 6.1 and 8.6. Let $\mathcal{N}_K \subset \mathcal{M}_K$ be the set of \mathcal{M}_K -primes inert in the extension $E\bar{E}GK/K$. Now let $\mathcal{Z}_K = \mathcal{N}_K \cup \mathcal{S}_K \cup \mathcal{T}_K$. This set can be infinite since it can contain all the primes inert in the cyclic extension $E\bar{E}GK/K$. It might also happen that some primes of \mathcal{T}_K or \mathcal{S}_K split in GK/K or divide the discriminant of $R(X)$. In this case we will have to use the fact that we can bound any finite set of primes in GK_∞ as in the totally real case. Now observe that minus this complication, \mathcal{Z}_K satisfies Notation and Assumptions 8.6 and thus the first assertion of the lemma follows.

- (2) This assertion of the lemma can be handled in almost the same way as the first assertion. Indeed suppose we start in $O_{GK_\infty, \mathcal{S}_{GK_\infty}}$ instead of $O_{GK_\infty, \mathcal{Z}_{GK_\infty}}$. Then the only difference will be that when we “descend” to K we will find ourselves in the ring O_{K, \mathcal{S}_K} . Thus, we can use Proposition 2.1 to take the “integer” route down to \mathbb{Z} without worrying about primes in \mathcal{T}_K .

□

If we assume additionally that the set of rational primes with 0 degree index with respect to K_∞ is infinite, then we have a simplified version of the statements above.

Theorem 8.10. Let K_∞ be a totally real possibly infinite algebraic extension of \mathbb{Q} , normal over some number field. Let U_∞ be a finite extension of K_∞ such that there exists an elliptic curve \mathbf{E} defined over U_∞ with $\mathbf{E}(U_\infty)$ finitely generated. Let GK_∞ be an extension of degree 2 over K_∞ . Assume that the set of rational primes with 0 degree index with respect to K_∞ is infinite and includes 2. Then for every $\varepsilon > 0$ there exists a number field $K \subset K_\infty$ and a set $\hat{\mathcal{Z}}_K \subset \mathcal{P}(K)$ of density (natural or Dirichlet) bigger than $1/2 - \varepsilon$ such that \mathbb{Z} is existentially definable and HTP is unsolvable in the integral closure of $O_{K, \hat{\mathcal{Z}}_K}$ in GK_∞ .

Proof. The proof of this part of the theorem is completely analogous to the proof of Theorem 11.8 of [33].

□

9. USING RANK ONE CURVES IN INFINITE EXTENSIONS.

In this section we will see to what extent we can duplicate the results in [17] and [18] over an infinite algebraic extension of \mathbb{Q} . Some of our assumptions and notation in this section will be different from the ones we used above.

Notation and Assumptions 9.1. The following assumptions and notation will be different or new in this section.

- Let K be a number field. (Note that we no longer assume that K is totally real.)
- Let K_∞ be an algebraic extension of K .
- Let E be an elliptic curve defined over K such that $\text{rank}(E(K)) = 1$ and $E(K_\infty) = E(K)$. (Note the new rank assumption.)
- Let Q be a generator of $E(K)$ modulo the torsion group.
- For a rational prime t let \mathbb{F}_t be a finite field of t elements.
- Let $p \neq q \in \mathcal{P}(\mathbb{Q}) \setminus \{2\}$. Let $\mathfrak{p}, \mathfrak{q}$ be K -primes above p and q respectively with $f(\mathfrak{p}/p) = f(\mathfrak{q}/q) = 1$. Assume additionally that $y_1(P) \not\equiv 0 \pmod{\mathfrak{p}}$ and $y_1(P) \not\equiv 0 \pmod{\mathfrak{q}}$ while integrality at \mathfrak{p} and \mathfrak{q} is definable in K_∞ .
- Let $M = \#E(\mathbb{F}_p)\#E(\mathbb{F}_q)pq$.

As we will see below we will be able to transfer almost seamlessly facts from the finite case to the infinite case. First we review some technical details of the original results in [17] and [18].

Theorem 9.2. *There exists a sequence of rational primes $\{\ell_i\}$, and sets $\mathcal{A}_K, \mathcal{B}_K \subset \mathcal{P}(K)$ satisfying the following properties.*

- (1) *The natural (and Dirichlet) density of \mathcal{A}_K and \mathcal{B}_K is 0.*
- (2) *$\mathcal{A}_K \cap \mathcal{B}_K = \emptyset$.*
- (3) *For any $\mathcal{W}_K \subset \mathcal{P}(K)$ such that $\mathcal{A}_K \subseteq \mathcal{W}_K$ and such that $\mathcal{W}_K \cap \mathcal{B}_K = \emptyset$ we have that $E(O_{K, \mathcal{W}_K}) = \{\pm \ell_i P : i \in \mathbb{Z}_{>0}\} \cup \{\text{finite set}\}$.*
- (4) *The set $\{x_{\ell_i}(Q) : i \in \mathbb{Z}_{>0}\}$ is discrete in every \mathfrak{p} -adic and archimedean topology of K .*

This theorem follows Lemma 3.10 and Proposition 3.15 of [18]. Now, given our assumptions on the behavior of E over K_∞ and the fact that any non-archimedean or archimedean topology of K_∞ must be an extension of the corresponding topology on K , we immediately obtain the following corollary.

Corollary 9.3. *There exists a sequence of rational primes $\{\ell_i\}$, and sets $\mathcal{A}_K, \mathcal{B}_K \subset \mathcal{P}(K)$ satisfying the following properties.*

- (1) *The natural (and Dirichlet) density of \mathcal{A}_K and \mathcal{B}_K is 0.*
- (2) *$\mathcal{A}_K \cap \mathcal{B}_K = \emptyset$.*
- (3) *For any $\mathcal{W}_K \subset \mathcal{P}(K)$ such that $\mathcal{A}_K \subseteq \mathcal{W}_K$ and such that $\mathcal{W}_K \cap \mathcal{B}_K = \emptyset$ we have that $E(O_{K_\infty, \mathcal{W}_K}) = \{\pm \ell_i P : i \in \mathbb{Z}_{>0}\} \cup \{\text{finite set}\}$.*
- (4) *The set $\{x_{\ell_i}(Q) : i \in \mathbb{Z}_{>0}\}$ is discrete in every \mathfrak{p} -adic and archimedean topology of K_∞ .*

We now proceed to another result in [18] which constructs (indirectly) a Diophantine model of $(\mathbb{Z}, +, \times)$ over O_{K, \mathcal{W}_K} , where \mathcal{W}_K will satisfy somewhat different conditions as will be described below. We start with a sequence of propositions from [18] (Lemma 3.16, Corollary 3.17, Lemma 3.20):

Lemma 9.4. *Let $B = \{2^n + n^2 : n \in \mathbb{Z}_{\geq 1}\}$. Then multiplication admits a positive existential definition in the structure $\mathcal{Z} := (\mathbb{Z}_{\geq 1}, 1, +, B)$. (Here B is considered as an unary predicate.)*

Corollary 9.5. *The structure $(\mathbb{Z}, 0, 1, +, \cdot)$ admits a positive existential model in the structure \mathcal{Z} .*

Lemma 9.6. *Let \mathfrak{t}, t stand for \mathfrak{p}, p or \mathfrak{q}, q respectively. Then if $m \in \mathbb{Z}_{\geq 1}$, we have that*

$$\text{ord}_{\mathfrak{t}}(x_{mM+1} - x_1) = \text{ord}_{\mathfrak{t}}(x_{M+1} - x_1) + \text{ord}_{\mathfrak{t}} m.$$

Proposition 9.7. *There exists a computable sequence of rational primes $\{\ell_i\}$, and sets $\mathcal{A}_K, \mathcal{B}_K \subset \mathcal{P}(K)$ satisfying the following properties.*

- (1) *The natural (and Dirichlet) density of \mathcal{A}_K and \mathcal{B}_K is 0.*
- (2) *$\mathcal{A}_K \cap \mathcal{B}_K = \emptyset$.*

- (3) For any $\mathcal{W}_K \subset \mathcal{P}(K)$ such that $\mathcal{A}_K \subseteq \mathcal{W}_K$ and such that $\mathcal{W}_K \cap \mathcal{B}_K = \emptyset$ we have that $\mathbf{E}(O_{K_\infty, \mathcal{W}_{K_\infty}}) = \mathbf{E}(O_{K, \mathcal{W}_K}) = \{\pm \ell_i P : i \in \mathbb{Z}_{>0}\} \cup \{\text{finite set}\}$.
- (4) The highest power of p dividing $(\ell_i - 1)/M$ is p^i , and $i \in B$ iff and only if q divides $(\ell_i - 1)/M$

Proposition 9.8. *Let $A := \{x_{\ell_1}, x_{\ell_2}, \dots\}$. Then A is a Diophantine model of \mathcal{Z} over $\mathcal{O}_{K_\infty, \mathcal{W}_{K_\infty}}$, via the bijection $\phi: \mathbb{Z}_{\geq 1} \rightarrow A$ taking i to x_{ℓ_i} .*

Proof. The set A is Diophantine over $\mathcal{O}_{K_\infty, \mathcal{W}_{K_\infty}}$ by Proposition 9.7. Further we have

$$\begin{aligned} i \in B &\iff q \text{ divides } (\ell_i - 1)/M && \text{(by Proposition 9.7 again)} \\ &\iff \text{ord}_q(x_{\ell_i} - x_1) > \text{ord}_q(x_{M+1} - x_1), \end{aligned}$$

by Lemma 9.6. The latter inequality is a Diophantine condition on x_{ℓ_i} over K_∞ by our assumption that integrality is definable at \mathfrak{q} over K_∞ . Thus the subset $\phi(B)$ of A is Diophantine over $\mathcal{O}_{K_\infty, \mathcal{W}_{K_\infty}}$.

Finally, for $i \in \mathbb{Z}_{\geq 1}$, Lemma 9.6 and assertion 4 of Proposition 9.7 imply $\text{ord}_{\mathfrak{p}}(x_{\ell_i} - x_1) = c + i$, where the integer $c = \text{ord}_{\mathfrak{p}}(x_{M+1} - x_1)$ is independent of i . Therefore, for $i, j, k \in \mathbb{Z}_{\geq 1}$, we have

$$i + j = k \iff \text{ord}_{\mathfrak{p}}(x_{\ell_i} - x_1) + \text{ord}_{\mathfrak{p}}(x_{\ell_j} - x_1) = \text{ord}_{\mathfrak{p}}(x_{\ell_k} - x_1) + c.$$

Since integrality at \mathfrak{p} is also definable over K_∞ by our assumptions, it follows that the graph of $+$ corresponds under ϕ to a subset of A^3 that is Diophantine over $\mathcal{O}_{K_\infty, \mathcal{W}_{K_\infty}}$. Thus A is a Diophantine model of \mathcal{Z} over $\mathcal{O}_{K_\infty, \mathcal{W}_{K_\infty}}$. \square

We can now combine Proposition 9.8 and Corollary 9.5 to obtain the main result of this section.

Theorem 9.9. *$\mathcal{O}_{K_\infty, \mathcal{W}_{K_\infty}}$ has Diophantine model of \mathbb{Z} and therefore HTP is undecidable over $\mathcal{O}_{K_\infty, \mathcal{W}_{K_\infty}}$.*

We summarize the discussion above in the following theorem.

Theorem 9.10. *Let K_∞ be an algebraic extension of \mathbb{Q} such that there exists an elliptic curve \mathbf{E} defined over K_∞ with $\mathbf{E}(K_\infty)$ of rank 1 and finitely generated. Fix a Weierstrass equation for \mathbf{E} and a number field K containing all the coefficients of the Weierstrass equation and the coordinates of all the generators of $\mathbf{E}(K_\infty)$. Assume that K has two odd relative degree one primes \mathfrak{p} and \mathfrak{q} such that integrality is definable at \mathfrak{p} and \mathfrak{q} over K_∞ .*

- (1) *There exist a set \mathcal{W}_K of K -primes of natural density 1 such that over $O_{K_\infty, \mathcal{W}_{K_\infty}}$ there exists an infinite Diophantine set simultaneously discrete in all archimedean and non-archimedean topologies of K_∞ .*
- (2) *There exist a set \mathcal{W}_K of K -primes of natural density 1 such that over $O_{K_\infty, \mathcal{W}_{K_\infty}}$ in K_∞ there exists a Diophantine model of \mathbb{Z} and therefore HTP is not solvable over $O_{K_\infty, \mathcal{W}_{K_\infty}}$.*

10. EXAMPLES

In this section we discuss some examples of elliptic curves and fields to which our results are applicable. Our primary source is [12]. Using Notation and Assumptions 5.1, let $K = \mathbb{Q}$ and let $F = \mathbb{Q}(\sqrt{-7})$. Let \mathbf{E} be the elliptic curve defined by the equation $y^2 + y = x^3 - x$. A direct calculation shows that this elliptic curve does not have complex multiplication. Let K_∞ be the unique cyclotomic \mathbb{Z}_5 extension of \mathbb{Q} . Then from the example in Section 1 of [12] we have that $\text{rank}(\mathbf{E}(FK_\infty)) = 1$, and by Proposition 4.8 the Mordell-Weil group of $\mathbf{E}(FK_\infty)$ is finitely generated. Further K_∞ has a totally real extension of degree 2. Thus by Theorem 5.4 and Theorem 7.9, \mathbb{Z} is existentially definable and HTP is unsolvable in the ring of integers of K_∞ and any extension of degree 2 of K_∞ .

We next consider the big ring situation. Observe that only one rational prime ramifies in K_∞ , K_∞ is Galois over K , and degrees of all the number fields contained in K_∞ are powers of 5. Thus, integrality is definable over K_∞ at all but finitely many primes by Corollary 2.4. Further, it then follows by Theorems 6.9, 6.13, 8.9, and 8.10 that for all small and some big subrings R of K_∞ or its arbitrary extension of degree 2, \mathbb{Z} is existentially definable and HTP is unsolvable over R . We must point out here that these conclusions concerning small and big rings (but not rings of integers) also follow from [33] since K_∞ is an abelian extension of \mathbb{Q} with finitely many ramified rational primes. Note also that the results concerning the ring of integers of K_∞ cannot be obtained directly from the theorem of Denef concerning infinite extensions

because it requires the elliptic curve of positive rank over \mathbb{Q} keeping the same rank in an infinite totally real extension.

Finally we can exploit the fact that the elliptic curve is of rank one in FK_∞ to conclude that FK_∞ has a “very large” ring R (i.e. a ring which is an integral closure of a big subring of a number field with the natural density of inverted primes equal to 1) which has a Diophantine model of \mathbb{Z} and unsolvable HTP.

11. APPENDIX

Lemma 11.1. *Let M be a number field. Let $z_1, z_2 \in M$ be such that $\mathfrak{d}_M(z_1)$ and $\mathfrak{d}_M(z_2)$ have no common factors. Then we can write $z_1 = \frac{a_1}{b_1}, z_2 = \frac{a_2}{b_2}$, where $a_1, a_2, b_1, b_2 \in O_M$, $(b_1, b_2) = 1$ in O_M and $(\mathfrak{n}_M(a_i), \mathfrak{d}_M(z_i)) = 1$.*

Proof. By the Strong Approximation Theorem there exists $b_1 \in O_M$ such that for any prime $\mathfrak{p} \in \mathcal{P}(M)$ occurring in $\mathfrak{d}_M(z_1)$ we have that $\text{ord}_{\mathfrak{p}} b_1 = \text{ord}_{\mathfrak{p}} \mathfrak{d}_M(z_1)$ and for any prime $\mathfrak{p} \in \mathcal{P}(M)$ occurring in $\mathfrak{d}_M(z_2)$, we have that $\text{ord}_{\mathfrak{p}} b_1 = 0$. Further, also by the Strong Approximation Theorem, there exists $b_2 \in O_M$ such that for any prime $\mathfrak{p} \in \mathcal{P}(M)$ occurring in $\mathfrak{d}_M(z_2)$ we have that $\text{ord}_{\mathfrak{p}} b_2 = \text{ord}_{\mathfrak{p}} \mathfrak{d}_M(z_2)$ and for any prime $\mathfrak{p} \in \mathcal{P}(M)$ such that $\text{ord}_{\mathfrak{p}} b_1 > 0$ we have that $\text{ord}_{\mathfrak{p}} b_2 = 0$. Now we have that $b_i z_i \in O_M$, $(b_1, b_2) = 1$ and $(\mathfrak{n}_M(a_i), \mathfrak{d}_M(z_i)) = 1$. \square

Lemma 11.2. *Let K be a number field. Let E, G be two non-trivial Galois extensions of K such that $([E : K], [G : K]) = 1$. Let \mathfrak{p}_K be a prime of K such that \mathfrak{p}_K does not have a degree one factor in E . Let \mathfrak{p}_G be the G -prime above \mathfrak{p}_K . Then \mathfrak{p}_G does not have a relative degree one factor in GE .*

Proof. Given our assumption on the degrees of the extensions involved, we have that $E \cap G = K$. Consequently, since both extensions are Galois, we conclude that E and G are linearly disjoint over K and therefore $[EG : G] = [E : K]$ and $[EG : G] = [G : K]$. Further by Lemma B.3.7 of [32] we have that EG/K is Galois and hence every factor \mathfrak{p}_G of \mathfrak{p}_K in G has the same number of factors, relative and ramification degrees in EG with all the three numbers dividing $[EG : G] = [G : K]$. Similarly, every factor \mathfrak{p}_E of \mathfrak{p}_K in E has the same number of factors, relative and ramification degrees in EG with all the numbers dividing $[EG : E] = [E : K]$. Let \mathfrak{p}_{EG} be an EG -factor of \mathfrak{p}_K . Let \mathfrak{p}_E and \mathfrak{p}_G lie below \mathfrak{p}_{EG} in E and G respectively. Then $f(\mathfrak{p}_{EG}/\mathfrak{p}_E)f(\mathfrak{p}_E/\mathfrak{p}_K) = f(\mathfrak{p}_{EG}/\mathfrak{p}_G)f(\mathfrak{p}_G/\mathfrak{p}_K)$. Further, $f(\mathfrak{p}_{EG}/\mathfrak{p}_E), f(\mathfrak{p}_G/\mathfrak{p}_K)$ are divisors of $[G : K]$ and thus are pairwise relatively prime to $f(\mathfrak{p}_{EG}/\mathfrak{p}_G), f(\mathfrak{p}_E/\mathfrak{p}_K)$ which are divisors of $[E : K]$. Therefore by the Fundamental Theorem of Arithmetic we have $f(\mathfrak{p}_E/\mathfrak{p}_K) = f(\mathfrak{p}_{EG}/\mathfrak{p}_G)$. By assumption we have that $f(\mathfrak{p}_E/\mathfrak{p}_K) > 1$, and therefore we also have that $f(\mathfrak{p}_{EG}/\mathfrak{p}_G) > 1$. \square

The following lemma is an expanded version of an argument from [19] and [21].

Lemma 11.3. *Let G be a number field. Let $x, y \in O_G$ be such that for some $d \in O_G$ we have that $x^2 - dy^2 = 1$. Let δ be an element of the algebraic closure of \mathbb{Q} be such that $\delta^2 = d$ and assume that $\xi = x - \delta y$ is a root of unity. Then $\xi^4 = 1$.*

Proof. Observe that ξ, ξ^{-1} and $x = \frac{\xi + \xi^{-1}}{2}$ are algebraic integers. This is however impossible unless ξ is rational or $\xi + \xi^{-1} = 0$, by Proposition 2.16 of [36]. Thus, $\xi^4 = 1$. \square

REFERENCES

- [1] Gunther Cornelissen, Thanases Pheidas, and Karim Zahidi. Division-ample sets and diophantine problem for rings of integers. *Journal de Théorie des Nombres Bordeaux*, 17:727–735, 2005.
- [2] Martin Davis. Hilbert’s tenth problem is unsolvable. *American Mathematical Monthly*, 80:233–269, 1973.
- [3] Martin Davis, Yuri Matiyasevich, and Julia Robinson. Hilbert’s tenth problem. Diophantine equations: Positive aspects of a negative solution. In *Proc. Sympos. Pure Math.*, volume 28, pages 323–378. Amer. Math. Soc., 1976.
- [4] Jan Denef. Hilbert’s tenth problem for quadratic rings. *Proc. Amer. Math. Soc.*, 48:214–220, 1975.
- [5] Jan Denef. Diophantine sets of algebraic integers, II. *Transactions of American Mathematical Society*, 257(1):227–236, 1980.
- [6] Jan Denef and Leonard Lipshitz. Diophantine sets over some rings of algebraic integers. *Journal of London Mathematical Society*, 18(2):385–391, 1978.
- [7] Serge Lang. *Algebraic Number Theory*. Addison Wesley, Reading, MA, 1970.
- [8] Yuri V. Matiyasevich. *Hilbert’s tenth problem*. Foundations of Computing Series. MIT Press, Cambridge, MA, 1993. Translated from the 1993 Russian original by the author, With a foreword by Martin Davis.

- [9] Barry Mazur. The topology of rational points. *Experimental Mathematics*, 1(1):35–45, 1992.
- [10] Barry Mazur. Questions of decidability and undecidability in number theory. *Journal of Symbolic Logic*, 59(2):353–371, June 1994.
- [11] Barry Mazur. Speculation about the topology of rational points: An up-date. *Asterisque*, 228:165–181, 1995.
- [12] Barry Mazur. Open problems regarding rational points on curves and varieties. In A. J. Scholl and R. L. Taylor, editors, *Galois Representations in Arithmetic Algebraic Geometry*. Cambridge University Press, 1998.
- [13] Barry Mazur and Karl Rubin. Elliptic curves and class field theory. In *Proceedings of the International Congress of Mathematicians, Vol. II (Beijing, 2002)*, pages 185–195, Beijing, 2002. Higher Ed. Press.
- [14] Thanases Pheidas. Hilbert’s tenth problem for a class of rings of algebraic integers. *Proceedings of American Mathematical Society*, 104(2):611–620, 1988.
- [15] Bjorn Poonen. Elliptic curves whose rank does not grow and Hilbert’s Tenth Problem over the rings of integers. Private Communication.
- [16] Bjorn Poonen. Using elliptic curves of rank one towards the undecidability of Hilbert’s Tenth Problem over rings of algebraic integers. In C. Fieker and D. Kohel, editors, *Algorithmic Number Theory*, volume 2369 of *Lecture Notes in Computer Science*, pages 33–42. Springer Verlag, 2002.
- [17] Bjorn Poonen. Hilbert’s Tenth Problem and Mazur’s conjecture for large subrings of \mathbb{Q} . *Journal of AMS*, 16(4):981–990, 2003.
- [18] Bjorn Poonen and Alexandra Shlapentokh. Diophantine definability of infinite discrete non-archimedean sets and diophantine models for large subrings of number fields. *Journal für die Reine und Angewandte Mathematik*, 2005:27–48, 2005.
- [19] Wolfgang A. Schmid. On the set of integral solutions of the Pell equation in number fields. *Aequationes Math.*, 71(1-2):109–114, 2006.
- [20] Harold Shapiro and Alexandra Shlapentokh. Diophantine relations between algebraic number fields. *Communications on Pure and Applied Mathematics*, XLII:1113–1122, 1989.
- [21] Parvati Shastri. Integral points on the unit circle. *J. Number Theory*, 91(1):67–70, 2001.
- [22] Alexandra Shlapentokh. Elliptic curves retaining their rank in finite extensions and Hilbert’s tenth problem. To appear in *Transactions of AMS*.
- [23] Alexandra Shlapentokh. Extension of Hilbert’s tenth problem to some algebraic number fields. *Communications on Pure and Applied Mathematics*, XLII:939–962, 1989.
- [24] Alexandra Shlapentokh. Diophantine classes of holomorphy rings of global fields. *Journal of Algebra*, 169(1):139–175, October 1994.
- [25] Alexandra Shlapentokh. Diophantine undecidability in some rings of algebraic numbers of totally real infinite extensions of \mathbb{Q} . *Annals of Pure and Applied Logic*, 68:299–325, 1994.
- [26] Alexandra Shlapentokh. Diophantine definability over some rings of algebraic numbers with infinite number of primes allowed in the denominator. *Inventiones Mathematicae*, 129:489–507, 1997.
- [27] Alexandra Shlapentokh. Defining integrality at prime sets of high density in number fields. *Duke Mathematical Journal*, 101(1):117–134, 2000.
- [28] Alexandra Shlapentokh. Hilbert’s tenth problem over number fields, a survey. In Jan Denef, Leonard Lipshitz, Thanases Pheidas, and Jan Van Geel, editors, *Hilbert’s Tenth Problem: Relations with Arithmetic and Algebraic Geometry*, volume 270 of *Contemporary Mathematics*, pages 107–137. American Mathematical Society, 2000.
- [29] Alexandra Shlapentokh. On diophantine definability and decidability in large subrings of totally real number fields and their totally complex extensions of degree 2. *Journal of Number Theory*, 95:227–252, 2002.
- [30] Alexandra Shlapentokh. A ring version of Mazur’s conjecture on topology of rational points. *International Mathematics Research Notices*, 2003:7:411–423, 2003.
- [31] Alexandra Shlapentokh. On diophantine definability and decidability in some infinite totally real extensions of \mathbb{Q} . *Transactions of AMS*, 356(8):3189–3207, 2004.
- [32] Alexandra Shlapentokh. *Hilbert’s Tenth Problem: Diophantine Classes and Extensions to Global Fields*. Cambridge University Press, 2006.
- [33] Alexandra Shlapentokh. Diophantine definability and decidability in the extensions of degree 2 of totally real fields. *Journal of Algebra*, 313(2):846–896, 2007.
- [34] Joseph Silverman. On the independence of Heegner points associated to distinct quadratic imaginary fields. arXiv:math.NT/0508259 v2 15 Aug 2005.
- [35] Joseph Silverman. *The Arithmetic of Elliptic Curves*. Springer Verlag, New York, New York, 1986.
- [36] Lawrence C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1982.

DEPARTMENT OF MATHEMATICS, EAST CAROLINA UNIVERSITY, GREENVILLE, NC 27858
 E-mail address: shlapentokha@ecu.edu
 URL: www.personal.ecu.edu/shlapentokha